On the Central Charge of a Factorizable Hopf Algebra

Yorck Sommerhäuser   Yongchang Zhu

Abstract

For a semisimple factorizable Hopf algebra over a field of characteristic zero, we show that the value that an integral takes on the inverse Drinfel'd element differs from the value that it takes on the Drinfel'd element itself at most by a fourth root of unity. This can be reformulated by saying that the central charge of the Hopf algebra is an integer. If the dimension of the Hopf algebra is odd, we show that these two values differ at most by a sign, which can be reformulated by saying that the central charge is even. We give a precise condition on the dimension that determines whether the plus sign or the minus sign occurs. To formulate our results, we use the language of modular data.

Contents

Introduction

In the first book of his "Vorlesungen über Zahlentheorie," which has been translated into English (cf. [41]), E. Landau discusses various proofs of a result by C. F. Gauß (cf. [28]) on the sign of a certain sum of n terms that we will later, in Paragraph 2.6, denote by $\mathfrak{G}$. In particular, he discusses a proof by I. Schur (cf. [70]) and a proof by F. Mertens (cf. [46]). As Landau points out, and this is confirmed by the original sources, the starting point of Schur's proof is, in the notation of Paragraph 2.6, an equation of the form $\mathfrak{G}\mathfrak{G}' = n$, where $\mathfrak{G}'$ is the sum of the reciprocal values, whereas the starting point of Mertens' proof is an equation of the form $\mathfrak{G}^2 = \pm n$, or alternatively, by comparison with the first equation, $\mathfrak{G}' = \pm\mathfrak{G}$.

Every semisimple factorizable Hopf algebra, or more generally every modular category, gives rise to numbers $\mathfrak{g}$ and $\mathfrak{g}'$ that are in many ways analogous to the Gaussian sum $\mathfrak{G}$ and the reciprocal sum $\mathfrak{G}'$. In fact, as we will discuss in Paragraph 4.4, both sets of numbers become equal for a suitable choice of the factorizable Hopf algebra, so that the results for Hopf algebras can be viewed as direct generalizations of the results for Gaussian sums. Therefore, looking at the above equations, the question arises whether we also have the equations $\mathfrak{g}\mathfrak{g}' = n$ and $\mathfrak{g}' = \pm\mathfrak{g}$. Proofs of the first of these two equations can be found in many places in the literature; we mention here only [3], Cor. 3.1.11, p. 52 and [73], Exerc. II.5.6, p. 116. For the second equation, less is known: A result known as Vafa's theorem implies that $\mathfrak{g}/\mathfrak{g}'$ is a root of unity (cf. [3], Thm. 3.1.19, p. 57). It is customary to write this quotient as an exponential of a parameter c called the central charge, using certain normalization conventions that we will explain in Paragraph 1.7. Working through these conventions, the fact that $\mathfrak{g}/\mathfrak{g}'$ is a root of unity translates into the condition that the central charge is a rational number, this fact being at least one of the reasons for the appearance of the word 'rational' in the term 'rational conformal field theory'.

However, the question that arose from the classical case above was whether we have $\mathfrak{g}' = \pm\mathfrak{g}$, which translates into the condition that the central charge is an even integer. The first main result of this article is that this is indeed the case if the dimension of the Hopf algebra is odd. We conjecture that the result still holds if the dimension of the Hopf algebra is even. But what we can prove, and this is the second main result of this article, is that we have $\mathfrak{g}^4 = \mathfrak{g}'^4$, which means for the central charge that it is an integer.

Let us be more specific. From the R-matrix of a semisimple factorizable Hopf algebra over a field of characteristic zero, we can derive a special element, the so-called Drinfel'd element u. The analogue of the Gaussian sum $\mathfrak{G}$ that we are considering is the number $\mathfrak{g} = \chi_R(u^{-1})$, where χ_R denotes the character of the regular representation. Note that in this situation χ_R can also be described as the unique two-sided integral that satisfies $\chi_R(1) = n$, where n denotes the dimension of the Hopf algebra. Similarly, the reciprocal Gaussian sum has the

form $\mathfrak{g}' = \chi_R(u)$. In the case where n is odd, our first main result is that $\mathfrak{g}' = \mathfrak{g}$ if $n \equiv 1 \pmod 4$, and $\mathfrak{g}' = -\mathfrak{g}$ if $n \equiv 3 \pmod 4$, so that $\mathfrak{g}^2 = \mathfrak{g}'^2$. We conjecture that this is still correct if n is even, but we can only prove that $\mathfrak{g}^4 = \mathfrak{g}'^4$ in this case, which is our second main result, both of which together form exactly the two parts of Theorem 4.3.

All these results can be stated and proved entirely within the Hopf algebra framework. However, we have chosen not to do this, but rather to take an axiomatic approach via modular data. This has at least three advantages: It is considerably more elementary, it makes clearer which properties are actually used to establish the results, and it facilitates the transfer of the results from the theory of Hopf algebras to related fields.

A modular datum essentially consists of two matrices that satisfy certain relations. Although these matrices and the relations between them pervade the entire literature on conformal field theory, it appears that the first systematic attempt to cast these properties into a set of simple axioms has been undertaken by T. Gannon (cf. [26], [27]). Our definition in Paragraph 1.1 is a minor variant of his. In particular, we have designed our definition in such a way that the two essential matrices can be rescaled rather arbitrarily, and we have given names to the matrices: We speak of the Verlinde matrix $\mathbf{S}$ and of the Dehn matrix $\mathbf{T}$. We have done this because the symbols used for them vary quite a bit over the literature, so that it appears inappropriate to speak of the S-matrix and the T-matrix, in particular as this usage is exactly opposite to the original conventions, as used for example by R. Fricke and F. Klein (cf. [40], § II.2.2, p. 209).

Instead of using natural numbers $1, 2, 3, \dots$ to index the rows and the columns of our matrices, we have used an abstract finite index set I. The reason for this is that the basic operation for modular data is to take their Kronecker product, and the corresponding new index set, the Cartesian product of the two old ones, is not canonically modeled on a string of natural numbers. This operation is important because it forms the basis of a generalized Witt group for modular data, and, as in the classical case, the Gaussian sum is a homomorphism with respect to this group structure. However, we do not elaborate on this aspect in the sequel, at least not in this article.

Properties of modular data that break the scalability are given special names: We call a modular datum normalized if the elements s_{oo} and t_o in the left upper corner of the Verlinde and the Dehn matrix are equal to 1. If the elements in the first column of the Verlinde matrix are positive integers, we call the modular datum integral. It is mainly this integrality property that distinguishes modular data coming from semisimple factorizable Hopf algebras from other modular data.

It is built into the axioms that every modular datum gives rise to a projective representation of the homogeneous modular group. By definition, rescaling the

Verlinde and the Dehn matrix does not change this projective representation. Now every projective representation of the modular group can be lifted to an ordinary linear representation; as we discuss in Paragraph 1.7, this is a direct consequence of the defining relations. To do this, however, we need to fix the scaling of the Verlinde and the Dehn matrix, which means that we have to choose two parameters, called the generalized rank D and the multiplicative central charge ℓ, a close relative of the additive central charge c considered above. A modular datum for which these two choices have been made is called an extended modular datum. As we illustrate in Paragraph 5.6 by an instructive example, the choice of these two parameters greatly affects the properties of the extended modular datum. After the two parameters have been chosen, they can be used to scale the Verlinde and the Dehn matrix correctly, so that we get an ordinary representation of the modular group; these correctly scaled matrices are called the homogeneous Verlinde matrix $\mathbf{S}'$ and the homogeneous Dehn matrix $\mathbf{T}'$. In this context, let us note that it is customary in the literature to require that the square of the parameter D is equal to n, the global dimension of the modular datum; however, the only property that is necessary for the lifting is the condition $D^4 = n^2$. For this reason, we distinguish in Paragraph 1.7 between a rank and a generalized rank.

These general aspects of modular data that we have just discussed form the contents of the preliminary Section 1. We do not claim any originality here; we have just rearranged known material in a way that suits our later needs. The first section that contains new results is Section 2. We begin by introducing three notions: We say what a congruence datum and a projective congruence datum is, and define a Galois datum to be an integral modular datum whose entries t_i of the Dehn matrix are compatible with a certain action of a Galois group described in Paragraph 1.4 via the compatibility condition $t_{\sigma.i} = \sigma^2(t_i)$. We then concentrate on the case where the exponent N is odd, and reach after several auxiliary steps our first main result, namely Theorem 2.5: If the exponent of a normalized integral modular datum is odd, we have $\mathfrak{g}' = \pm\mathfrak{g}$. If the global dimension n of the modular datum is also odd, then we can sharpen this assertion and obtain, by comparing with the classical Gaussian sum $\mathfrak{G}$, the result that $\mathfrak{g}' = \mathfrak{g}$ if $n \equiv 1 \pmod 4$ and $\mathfrak{g}' = -\mathfrak{g}$ if $n \equiv 3 \pmod 4$, which is stated in Theorem 2.6. Recall that for Hopf algebras, which are still our main concern, it is a special case of Cauchy's theorem (cf. [37], Thm. 3.4, p. 26) that n is odd if and only if N is odd. If we extend the modular datum using a rank, then Theorem 2.6 means for the corresponding additive central charge c that it is an even integer satisfying $c \equiv 0 \pmod 4$ if $n \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 4$ if $n \equiv 3 \pmod 4$.

In Section 3, we turn to the case where N is even. Our main tool here is a result by F. R. Beyl, which we quote in Paragraph 3.1 and which asserts that the Schur multiplicator of the reduced modular group $\mathrm{SL}(2, \mathbb{Z}_N)$ is either trivial or isomorphic to $\mathbb{Z}_2$. As we explain, it follows from this that, in contrast to the case of the unreduced modular group considered above, projective representations of

the reduced modular group cannot always be completely lifted to an ordinary representation, but can be lifted up to a sign. In fact, we will see a nice explicit example of this phenomenon in Paragraph 5.6. From Beyl's result and a couple of auxiliary steps, we deduce in Theorem 3.4 that, for a normalized extended projective congruence datum that is also Galois, we have $\mathfrak{g}^4 = \mathfrak{g}'^4$. For the multiplicative central charge, this means that $\ell^{24} = 1$, which in turn means that the additive central charge c is an integer. As the example just mentioned also shows, the conclusion of this theorem cannot be sharpened to the assertion that $\mathfrak{g}^2 = \mathfrak{g}'^2$, as in the case of odd exponents. However, in the case of Hopf algebras, we conjecture that it can be sharpened in this way.

It is very important to emphasize that the same result, the integrality of c, has been already derived before by A. Coste and T. Gannon from assumptions that look, and are, very similar (cf. [11], § 2.4, Prop. 3.b, p. 9). Their argument is short and elegant, and we also use it as a part of our proof, as the reader will confirm when looking at Lemma 2.3. However, in the preceding terminology, Coste and Gannon impose the Galois condition on the homogeneous Dehn matrix $\mathbf{T}'$, whereas we, having the applications to Hopf algebras in mind, impose it on the original Dehn matrix $\mathbf{T}$. To deduce their assumption from ours is therefore exactly equivalent to proving our result, as we explain in greater detail in Paragraph 3.4.

Section 3 ends with some results on the relation of the prime divisors of N and the prime divisors of n. This is, of course, inspired by Cauchy's theorem for Hopf algebras mentioned above. In Corollary 3.5, we prove in particular that, for a projective congruence datum that is also Galois, we have $N \equiv 0 \pmod 4$ if $n \equiv 2 \pmod 4$. We do not think, however, that this result is the best possible one, and close the section with a conjecture about a potential improvement.

Finally, we apply in Section 4 all the machinery developed before to Hopf algebras. What we consider are semisimple factorizable Hopf algebras over fields of characteristic zero, which lead, as we explain, via the Drinfel'd element u to modular categories and integral modular data. The application of the preceding results is now rather straightforward. If the dimension n of the Hopf algebra is odd, Cauchy's theorem and Theorem 2.6 now yield that $\chi_R(u) = \chi_R(u^{-1})$ if $n \equiv 1 \pmod 4$ and $\chi_R(u) = -\chi_R(u^{-1})$ if $n \equiv 3 \pmod 4$. On the other hand, if n is even, Theorem 3.4 yields that $\chi_R(u)^4 = \chi_R(u^{-1})^4$. Of course, we have to verify the rather strong assumptions of this theorem, but here we can rely on earlier work: That we are working with a projective congruence datum follows from the projective congruence subgroup theorem for Hopf algebras (cf. [68], Thm. 9.4, p. 94), and it is also known that our modular datum is Galois (cf. [68], Lem. 12.2, p. 115). All these results are obtained in Paragraph 4.3, where we also state explicitly our conjecture that the equation $\chi_R(u)^2 = \chi_R(u^{-1})^2$ also holds in the case of an even-dimensional Hopf algebra. We also expect that the dimension of such an even-dimensional semisimple factorizable Hopf algebra is always divisible by 4.

At the end of Section 4, we discuss an example that was constructed originally by D. E. Radford (cf. [60], Sec. 3, p. 10; [61], Sec. 2.1, p. 219). In this example, the group ring of a cyclic group of odd order n is endowed with a nonstandard R-matrix based on a primitive n-th root of unity. For this R-matrix, the Gaussian sum $\mathfrak{g}$ becomes the classical Gaussian sum $\mathfrak{G}$, which shows that our preceding considerations really are generalizations of the classical case.

In the same way as Hopf algebras, quasi-Hopf algebras lead to modular data, and these are also integral if their ribbon element is chosen correctly. Therefore, our methods apply in just the same way, as we discuss in Section 5. However, our results in the case of a quasi-Hopf algebra are less strong, which is due to the fact that, although the projective congruence subgroup theorem has been carried over to quasi-Hopf algebras (cf. [57], Thm. 8.8, p. 35), the Galois property of the corresponding modular datum has not yet been established. We are, however, optimistic that this will happen in the near future, and then our methods can be used to deduce that we have $\mathfrak{g}^4 = \mathfrak{g}'^4$ also in the quasi-Hopf algebra case. But this result can, and this is the main point of the discussion, not be improved: We construct an explicit example of a quasi-Hopf algebra for which $\mathfrak{g}^2 \neq \mathfrak{g}'^2$. As we mentioned above, we conjecture that it is impossible to construct such an example with an ordinary Hopf algebra.

Both this quasi-Hopf algebra and the arising modular datum have been considered before several times; however, we think that at least explicitly the connection between the two has not been made so far. Using a term from [63], we call the modular datum the semion datum; it is usually constructed using affine Kac-Moody algebras, and there is a particularly simple case. The quasi-Hopf algebra that we are using is a dual group ring, endowed with a nontrivial associator with the help of a 3-cocycle, a construction that has also been used frequently, also in the particularly simple case of a group of order 2, as we confirm by giving several explicit references. The fact that this quasi-Hopf algebra leads to the semion datum means that practically all our conjectures for Hopf algebras are false for quasi-Hopf algebras: Besides the fact that $\mathfrak{g}^2 \neq \mathfrak{g}'^2$ already mentioned, the semion datum is a projective congruence datum that is not a congruence datum in the sense of Definition 2.1. The semion datum also shows that the congruence properties explicitly depend on how the modular datum is extended by the choice of a generalized rank and a multiplicative central charge, and, as mentioned above, it provides an explicit projective representation of a reduced modular group that cannot be lifted to a linear representation, thus confirming the nontriviality of the corresponding Schur multiplicator.

Finally, let us say some words about the conventions that we use throughout the exposition. Our base field is denoted by K, and while we always assume that it is of characteristic zero, we do not always assume that it is algebraically closed. The dual of a vector space V is denoted by $V^* := \operatorname{Hom}_K(V, K)$. Unless stated otherwise, a module is a left module. If R is a ring, then $R^\times$ denotes its group of units. Also, we use the so-called Kronecker symbol δ_{ij}, which is equal to 1 if $i = j$ and equal to 0 otherwise. The set of natural numbers is the set $\mathbb{N} := \{1, 2, 3, \ldots\}$;

in particular, 0 is not a natural number. The symbol $\mathbb{Q}_N$ denotes the N-th cyclotomic field, and not some field of N-adic numbers, and $\mathbb{Z}_N$ denotes the set $\mathbb{Z}/N\mathbb{Z}$ of integers modulo N, and not some ring of N-adic integers. The greatest common divisor of two integers k and l is denoted by $\gcd(k, l)$ and is always chosen to be nonnegative. With respect to enumeration, we use the convention that propositions, definitions, and similar items are referenced by the paragraph in which they occur; an additional third digit indicates a part of the corresponding item. For example, a reference to Proposition 1.1.1 refers to the first assertion of the unique proposition in Paragraph 1.1.

1 Preliminaries

1.1 Although modular data have played a very prominent role in conformal field theory for quite some time, it appears that the approach to derive their properties from a set of simple axioms was first proposed by T. Gannon (cf. [26], Def. 1, p. 214; [27], Def. 6.1.6, p. 359). We use here a slight modification of his system of axioms; the relation of the two systems of axioms will become clear in Paragraph 1.7.

Definition Suppose that K is a field of characteristic zero. A modular datum over K is a quintuple $(I, o, {}^*, \mathbf{S}, \mathbf{T})$ consisting of a finite set I, a distinguished element $o \in I$, called the unit element, an involution

$$^* : I \to I, \ i \mapsto i^*$$

a matrix $\mathbf{S} = (s_{ij})_{i,j \in I}$ with entries in K, called the Verlinde matrix, and a diagonal matrix $\mathbf{T} = (t_i \delta_{ij})_{i,j \in I}$ with entries in K, called the Dehn matrix. We require these to satisfy the following axioms:

1. $\mathbf{S}$ is symmetric, and $\mathbf{T}$ has finite order.

2. For all $i \in I$, we have $t_{i^*} = t_i$ and $s_{io} \neq 0$. Moreover, we have $o^* = o$.

3. There is a nonzero number $n \in K$ such that

$$\sum_{j \in I} s_{ij} s_{jk} = n \delta_{i,k^*}$$

   for all $i, k \in I$.

4. The matrices $\mathbf{T}^{-1} \mathbf{S} \mathbf{T}^{-1}$ and $\mathbf{S} \mathbf{T} \mathbf{S}$ are proportional.

5. The numbers

$$N_{i,j}^k := \frac{1}{n} \sum_{l \in I} \frac{s_{il} s_{jl} s_{k^* l}}{s_{ol}}$$

   are nonnegative integers.

A modular datum is called normalized if $s_{oo} = t_o = 1$. It is called integral if the elements s_{io} are positive integers.

When we refer to elements of the base field K as integers, what we really mean is that this field element is the image of an integer under the unique field isomorphism between $\mathbb{Q}$ and the prime field of K. In the sequel, we will frequently pass in this way from a rational number to a field element and vice versa without explicit mention.

Note that, with the exception of normality and integrality, the axioms of a modular datum have the property that they are still satisfied if we rescale the Verlinde matrix by a nonzero factor and the Dehn matrix by a root of unity.

The various constants that appear in this definition have special names. If $\mathbf{E} = (\delta_{ij})_{i,j \in I}$ is the unit matrix, then the definition implies that there is a smallest number N, called the exponent of the modular datum, such that $\mathbf{T}^N = \mathbf{E}$. The diagonal entries t_i of the Dehn matrix are then N-th roots of unity. The normalized Dehn matrix $\mathbf{T}/t_o$ then also has finite order, so that there is a smallest number N_o, called the normalized exponent of the modular datum, such that $(\mathbf{T}/t_o)^{N_o} = \mathbf{E}$. Clearly, N_o divides N.

The number n appearing in Axiom 3 is called the global dimension of the modular datum. Inserting $i = k = o$ into this axiom, we get that $n = \sum_{j \in I} s_{jo}^2$. For $i \in I$, we also call the number $n_i := s_{io}$ the i-th dimension, so that we can reformulate the last equation as $\sum_{j \in I} n_j^2 = n$. If we introduce the charge conjugation matrix $\mathbf{C} := (\delta_{i,j^*})_{i,j \in I}$, then Axiom 3 can be written in the matrix form $\mathbf{S}^2 = n\mathbf{C}$. Since $n \neq 0$, we see in particular that both $\mathbf{S}$ and $\mathbf{T}$ are invertible. Note also that the integrality condition means that the dimensions n_i are positive integers, and therefore the global dimension n is also a positive integer. In this context, let us point out that our definition of integrality deviates from the one in [14], Def. 3.1, where in particular all entries of the Verlinde matrix are required to be integers.

We can also determine the proportionality constant in Axiom 4. The (o, o)-component of $\mathbf{STS}$ is the so-called Gaussian sum $\mathfrak{g} := \sum_{i \in I} n_i^2 t_i$ of the modular datum, whereas the (o, o)-component of $\mathbf{T}^{-1}\mathbf{ST}^{-1}$ is n_o/t_o^2, so that Axiom 4 becomes

$$\mathfrak{g}\mathbf{T}^{-1}\mathbf{ST}^{-1} = \frac{n_o}{t_o^2}\mathbf{STS}$$

which we will call the constant form of Axiom 4.

We list some elementary consequences of our axioms that will be frequently used in the sequel:

Proposition
1. We have $s_{i^*,j^*} = s_{ij}$ and $n_{j^*} = n_j$.

2. The matrix $\mathbf{C}$ commutes with $\mathbf{S}$ and $\mathbf{T}$; i.e., we have $\mathbf{CS} = \mathbf{SC}$ and $\mathbf{CT} = \mathbf{TC}$.

3. For all $i, j \in I$, we have $N_{oi}^j = N_{io}^j = \delta_{ij}$ and $N_{ij}^o = \delta_{i,j^*}$.

4. For all $i, j \in I$, we have

$$s_{ij} = \frac{t_o}{t_i t_j} \sum_{k \in I} N_{ik}^j n_k t_k$$

5. We have $\mathfrak{g}\mathfrak{g}' = nn_o^2$, where $\mathfrak{g}' := \sum_{i \in I} \frac{n_i^2}{t_i}$ is the so-called reciprocal Gaussian sum. In particular, the Gaussian sum and its reciprocal are nonzero.

Proof. (1) Written in matrix form, the first part of the first assertion says that $\mathbf{CSC} = \mathbf{S}$, or alternatively $\mathbf{CS} = \mathbf{SC}$. But this holds since $\mathbf{C} = \frac{1}{n}\mathbf{S}^2$. Setting $i = o$ gives the second part of the first assertion. For the second assertion, we have just seen that $\mathbf{S}$ commutes with $\mathbf{C}$, and the fact that $\mathbf{T}$ commutes with $\mathbf{C}$ is equivalent to our axiom that $t_{i^*} = t_i$. The third assertion is a direct consequence of Axiom 3.

(2) For the fourth assertion, the (o,l)-component of the constant form of Axiom 4 yields

$$\frac{\mathfrak{g}n_l}{t_o t_l} = \frac{n_o}{t_o^2} \sum_{j \in I} n_j t_j s_{jl}$$

Using the definition of the numbers N_{ij}^k, we therefore get

$$\sum_{j \in I} N_{ij}^k n_j t_j = \frac{1}{n} \sum_{j,l \in I} \frac{s_{il} s_{jl} s_{k^*l}}{n_l} n_j t_j = \frac{t_o \mathfrak{g}}{n n_o} \sum_{l \in I} s_{il} s_{k^*l} \frac{1}{t_l} = \frac{t_i t_k}{t_o} s_{ik}$$

where the last step uses the matrix identity $\mathfrak{g}\mathbf{S}^{-1}\mathbf{T}^{-1}\mathbf{S} = \frac{n_o}{t_o^2}\mathbf{TST}$.

(3) For the fifth assertion, we first note that the Gaussian sum is clearly nonzero, because the right-hand side in the constant form of Axiom 4 is invertible. If we invert this very equation, it becomes

$$\frac{1}{\mathfrak{g}}\mathbf{TS}^{-1}\mathbf{T} = \frac{t_o^2}{n_o}\mathbf{S}^{-1}\mathbf{T}^{-1}\mathbf{S}^{-1}$$

As we have $\mathbf{S}^{-1} = \frac{1}{n}\mathbf{SC}$, we can write this in the form

$$\frac{1}{\mathfrak{g}}\mathbf{TSCT} = \frac{t_o^2}{nn_o}\mathbf{ST}^{-1}\mathbf{S}$$

The (o,o)-component of this matrix equation is

$$\frac{t_o^2 n_o}{\mathfrak{g}} = \frac{t_o^2}{nn_o} \sum_{i \in I} s_{oi} \frac{1}{t_i} s_{io} = \frac{t_o^2}{nn_o}\mathfrak{g}'$$

which yields the fifth assertion. $\square$

Note that variants of the fourth assertion appear in [26], Sec. 4, p. 232 and [73], Sec. II.4.5, p. 108. The fifth assertion should be compared with [73], Sec. II.2.4, Eq. (2.4.a), p. 83, and Exerc. II.5.6, p. 116. As mentioned in the introduction, the fifth assertion gives a first relation between the Gaussian sum and its reciprocal; the main issue in this article will be to find more such relations.

1.2 With every modular datum, we associate a ring $\mathcal{F}$, called the fusion ring, as follows: As an abelian group, $\mathcal{F}$ is free on a basis $\{b_i \mid i \in I\}$. The multiplication is given on basis elements by

$$b_i b_j = \sum_{k \in I} N_{ij}^k b_k$$

and then on the whole group by bilinear extension. We will also frequently extend the scalars to other commutative rings R by considering $\mathcal{F}_R := \mathcal{F} \otimes_{\mathbb{Z}} R$.

As we have $N_{ij}^k = N_{ji}^k$ by construction, $\mathcal{F}$ is clearly commutative, and it follows from Proposition 1.1.3 that b_o is a unit element. But this multiplication is actually also associative, as we will show now. For this, we define for each $q \in I$ a group homomorphism $\xi_q : \mathcal{F} \to K$ to the additive group of the field by requiring that the value on the basis elements be

$$\xi_q(b_i) = \frac{s_{iq}}{n_q}$$

This map is not only a group homomorphism:

Lemma ξ_q is a ring homomorphism.

Proof. By Axiom 1.1.3 and Axiom 1.1.5, we have

$$\xi_q(b_i b_j) = \sum_{k \in I} N_{ij}^k \frac{s_{kq}}{n_q} = \frac{1}{n} \sum_{k,l \in I} \frac{s_{il} s_{jl} s_{k^*l}}{n_l} \frac{s_{kq}}{n_q}$$

$$= \sum_{l \in I} \frac{s_{il} s_{jl} \delta_{ql}}{n_l n_q} = \frac{s_{iq}}{n_q} \frac{s_{jq}}{n_q} = \xi_q(b_i)\xi_q(b_j)$$

where we have also used Proposition 1.1.1 for the third equality. The fact that $\xi_q(b_o) = 1$ follows directly from the definition. $\square$

Via this lemma, the associativity of $\mathcal{F}$ follows essentially from the associativity of K:

Proposition $\mathcal{F}$ is a commutative, associative, reduced ring with unit element b_o. The algebra $\mathcal{F}_{\mathbb{Q}}$ is semisimple.

Proof. If K^I denotes the algebra of functions on I with pointwise addition and multiplication, then it follows from the preceding lemma that the map

$$\mathcal{F} \to K^I, \ b \mapsto (\xi_i(b))_{i \in I}$$

is a ring homomorphism. Because the Verlinde matrix is invertible, this map is injective, and the map from $\mathcal{F}_K$ to K^I given by extension of scalars is in fact an algebra isomorphism. Since K^I is associative and reduced, this also holds for $\mathcal{F}$. Finally, it is a general fact that a finite-dimensional commutative reduced algebra over a field is semisimple (cf. [22], Thm. 2.2, p. 60). $\square$

The algebra isomorphism between $\mathcal{F}_K$ and K^I appearing in the preceding proof can be used to transfer all properties from K^I to $\mathcal{F}_K$; in particular, we can easily write down the primitive idempotents of $\mathcal{F}_K$. For this, we introduce the element

$$b_A := \sum_{j \in I} b_j b_{j^*}$$

which relates to the primitive idempotents as follows:

Corollary

1. For $i \in I$, we have $\xi_i(b_A) = \frac{n}{n_i^2} \neq 0$.

2. The element $p_i := \frac{1}{\xi_i(b_A)} \sum_{j \in I} \xi_i(b_{j^*}) b_j$ is a primitive idempotent in $\mathcal{F}_K$.

3. For $i, j \in I$, we have $\xi_j(p_i) = \delta_{ij}$.

4. For $b \in \mathcal{F}_K$, we have $b p_i = \xi_i(b) p_i$.

Proof. As we have $\xi_i(b_j) = \frac{s_{ij}}{n_i}$, it follows from Axiom 1.1.3 that

$$\xi_i(b_A) = \sum_{j \in I} \frac{s_{ij}}{n_i} \frac{s_{ij^*}}{n_i} = \frac{1}{n_i^2} \sum_{j \in I} s_{ij} s_{ji^*} = \frac{n}{n_i^2}$$

where we have also used Proposition 1.1.1. This proves the first assertion. For the following assertions, we should first point out that we have denoted the basis element $b_j \otimes 1 \in \mathcal{F}_K = \mathcal{F} \otimes_{\mathbb{Z}} K$ again by b_j, and also denoted the K-linear extension of ξ_i from $\mathcal{F}_K$ to K again by ξ_i. The third assertion then holds because

$$\xi_j(p_i) = \frac{1}{\xi_i(b_A)} \sum_{k \in I} \xi_i(b_{k^*}) \xi_j(b_k) = \frac{n_i^2}{n} \sum_{k \in I} \frac{s_{ik^*}}{n_i} \frac{s_{jk}}{n_j} = \delta_{ij}$$

by Axiom 1.1.3 and Proposition 1.1.1.

For the second assertion, we denote the algebra isomorphism appearing in the proof of the preceding proposition by $f : \mathcal{F}_K \to K^I$, $b \mapsto (\xi_j(b))_{j \in I}$. It follows from the third assertion that $f(p_i) = (\delta_{ij})_{j \in I}$, which is a primitive idempotent in K^I. Therefore, p_i must be a primitive idempotent in $\mathcal{F}_K$. The fourth assertion follows similarly: We have

$$f(b p_i) = f(b) f(p_i) = (\xi_j(b))_{j \in I} \, (\delta_{ij})_{j \in I} = \xi_i(b) \, (\delta_{ij})_{j \in I} = \xi_i(b) f(p_i)$$

and therefore $b p_i = \xi_i(b) p_i$. □

The special case $i = o$ of the fourth assertion in this corollary is worth noting: Since $\xi_o(b_j) = n_j / n_o$, we have $p_o = \frac{n_o}{n} \sum_{j \in I} n_j b_j$, and the fourth assertion then yields that $b_k p_o = \frac{n_k}{n_o} p_o$ for all $k \in I$.

It must be emphasized that the material in this paragraph is not at all new; it can be found in many places, among them [10], Def. 5.2.8, p. 155; [26], Def. 2,

14

p. 216; and [27], Def. 6.1.3, p. 355. An analogous discussion in the Hopf algebra case can be found in [68], Par. 5.1 and Par. 5.3. It is also worth noting that the rescaled Verlinde and Dehn matrices lead to the same fusion ring, as only homogeneous ratios of the matrix elements enter into the definition.

1.3 By construction, the diagonal elements t_i of the Dehn matrix generate the N-th cyclotomic field $\mathbb{Q}_N \subset K$, and the ratios t_i/t_o generate its subfield $\mathbb{Q}_{N_o}$. If the modular datum is integral, then we see by multiplying and dividing the right-hand side of the formula in Proposition 1.1.4 by t_o that the entries of the Verlinde matrix are in fact contained in $\mathbb{Q}_{N_o}$. This has the following consequence:

Proposition For an integral modular datum, the algebra $\mathcal{F}_{\mathbb{Q}}$ is isomorphic to a direct sum of subfields of the cyclotomic field $\mathbb{Q}_{N_o}$.

Proof. By the Wedderburn structure theorem (cf. [22], Thm. 1.11, p. 40), we can decompose $\mathcal{F}_{\mathbb{Q}}$ in the form

$$\mathcal{F}_{\mathbb{Q}} = \bigoplus_{q=1}^{r} K_q$$

where $K_1, \ldots, K_r$ are fields. As we saw in Paragraph 1.2, the algebra homomorphism $\mathcal{F}_{\mathbb{Q}} \to K^I$, $b \mapsto (\xi_i(b))_{i \in I}$ is injective. Therefore, for every $q \leq r$ there is an $i \in I$ such that $\xi_i(K_q)$ is nonzero. But as $\xi_i(b_j) = s_{ji}/n_i \in \mathbb{Q}_{N_o}$, the image of ξ_i is contained in $\mathbb{Q}_{N_o}$. Since field homomorphisms are always injective, ξ_i restricts to an isomorphism between K_q and a subfield of $\mathbb{Q}_{N_o}$. $\square$

The preceding argument should be compared with [15], App. B, p. 302, where a similar result is proved using the Kronecker-Weber theorem. Our argument also shows that the algebra homomorphisms ξ_i arise from the Wedderburn decomposition by projecting to a Wedderburn component K_q and then embedding it into $\mathbb{Q}_{N_o}$: Because the product of elements in distinct Wedderburn components is zero, and $\mathbb{Q}_{N_o}$ does not contain nontrivial zero divisors, every ξ_i must vanish on all Wedderburn components K_q except one, and on this Wedderburn component it becomes an embedding into $\mathbb{Q}_{N_o}$.

The maps ξ_i actually exhaust all algebra homomorphisms from $\mathcal{F}_{\mathbb{Q}}$ to $\mathbb{Q}_{N_o}$. This follows from Dedekind's theorem (cf. [32], § 1.3, Thm. 3, p. 25), which implies that distinct algebra homomorphisms are linearly independent elements in the vector space $\operatorname{Hom}_{\mathbb{Q}}(\mathcal{F}_{\mathbb{Q}}, \mathbb{Q}_{N_o})$ over $\mathbb{Q}_{N_o}$, whose dimension is the cardinality of I. Because the Verlinde matrix is invertible, it cannot have two proportional columns, which implies that the maps ξ_i are all distinct.

1.4 For an integral modular datum, consider the Galois group $\operatorname{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ of the cyclotomic field $\mathbb{Q}_{N_o}$. We have seen in Proposition 1.3 that the Wedderburn

components K_q in the Wedderburn decomposition

$$\mathcal{F}_{\mathbb{Q}} = \bigoplus_{q=1}^{r} K_q$$

are fields that can be embedded into $\mathbb{Q}_{N_o}$. Because the Galois group $\mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ is abelian, all subfields of $\mathbb{Q}_{N_o}$ are invariant under its action, and therefore we get an action of the Galois group on K_q, which for the same reason does not depend on the choice of the embedding. By summing up the actions on all the Wedderburn components, we get an action of $\mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ on $\mathcal{F}_{\mathbb{Q}}$, which has the property that

$$\xi_i(\sigma.b) = \sigma(\xi_i(b))$$

for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$, all $i \in I$, and all $b \in \mathcal{F}_{\mathbb{Q}}$. This holds because we saw in Paragraph 1.3 that the algebra homomorphisms ξ_i are exactly those which arise by projecting to some Wedderburn component and then embedding it into $\mathbb{Q}_{N_o}$.

Now $\sigma \circ \xi_i$ is again an algebra homomorphism from $\mathcal{F}_{\mathbb{Q}}$ to $\mathbb{Q}_{N_o}$, and therefore there must be an index $j \in I$ such that $\sigma \circ \xi_i = \xi_j$. We denote this index j by $\sigma.i$, and get in this way an action of $\mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ on the index set I with the property that

$$\sigma(\xi_i(b)) = \xi_{\sigma.i}(b)$$

for all $b \in \mathcal{F}_{\mathbb{Q}}$. The following proposition lists the basic properties of the actions that we have introduced:

Proposition For an integral modular datum, we have

1. $\sigma(s_{ij}) = s_{\sigma.i,j} = s_{i,\sigma.j}$

2. $n_i = n_{\sigma.i}$

3. $\sigma.b_i = b_{\sigma.i}$

4. $\sigma.o = o$

Proof. (1) From Corollary 1.2, we get that

$$\frac{n}{n_{\sigma.i}^2} = \xi_{\sigma.i}(b_A) = \sigma(\xi_i(b_A)) = \sigma(\frac{n}{n_i^2}) = \frac{n}{n_i^2}$$

This implies $n_{\sigma.i}^2 = n_i^2$, which implies $n_{\sigma.i} = n_i$ because every n_i is a positive integer by assumption. This proves the second assertion.

(2) By definition, we have $\xi_i(b_j) = \frac{s_{ij}}{n_i}$, so that the preceding equation implies

$$\frac{s_{\sigma.i,j}}{n_{\sigma.i}} = \xi_{\sigma.i}(b_j) = \sigma(\frac{s_{ij}}{n_i}) = \frac{\sigma(s_{ij})}{n_i}$$

16

This implies $\sigma(s_{ij}) = s_{\sigma.i,j}$ by the preceding step. By the symmetry of the Verlinde matrix, we then also have

$$\sigma(s_{ij}) = \sigma(s_{ji}) = s_{\sigma.j,i} = s_{i,\sigma.j}$$

which proves the first assertion.

(3) The equation $\sigma.b_i = b_{\sigma.i}$ will hold if we can show that $\xi_j(\sigma.b_i) = \xi_j(b_{\sigma.i})$ for all $j \in I$. But this equation holds, as we have

$$\xi_j(\sigma.b_i) = \sigma(\xi_j(b_i)) = \sigma(\frac{s_{ji}}{n_j}) = \frac{s_{j,\sigma.i}}{n_j} = \xi_j(b_{\sigma.i})$$

(4) By construction, σ acts as a unital algebra automorphism on $\mathcal{F}_{\mathbb{Q}}$, and in particular preserves the unit element, so that $\sigma.b_o = b_o$. By the preceding step, this implies $\sigma.o = o$. $\square$

Because N_o divides N, $\mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ is a factor group of $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, which implies that $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ also acts on I via pullback along the canonical map. This fact will be used in the sequel without explicit mention, for example in Definition 2.1.3.

1.5   The Galois group $\mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ contains an element γ that maps every N_o-th root of unity to its inverse. It corresponds to complex conjugation under every embedding of the cyclotomic field into the complex numbers. As we show now, this automorphism γ acts on the index set as the involution that is part of the definition of our modular datum, which is still assumed to be integral:

Proposition   For all $i \in I$, we have $\gamma.i = i^*$.

Proof.   Note first that from Proposition 1.1.1 we get

$$N_{i^*j^*}^{k^*} = \frac{1}{n} \sum_{l \in I} \frac{s_{i^*l} s_{j^*l} s_{kl}}{n_l} = \frac{1}{n} \sum_{l \in I} \frac{s_{i^*l^*} s_{j^*l^*} s_{kl^*}}{n_{l^*}} = \frac{1}{n} \sum_{l \in I} \frac{s_{il} s_{jl} s_{k^*l}}{n_l} = N_{ij}^k$$

which shows that the $\mathbb{Q}$-linear endomorphism of $\mathcal{F}_{\mathbb{Q}}$ that maps the basis element b_i to b_{i^*} is an algebra homomorphism. We extend this map antilinearly to the complexification $\mathcal{F}_{\mathbb{C}}$; i.e., for an element $x = \sum_{i \in I} z_i b_i$, with $z_i \in \mathbb{C}$, we define

$$x^* = \sum_{i \in I} \bar{z}_i b_{i^*}$$

where $\bar{z}_i$ is the complex conjugate of z_i.

The basis $\{b_i \mid i \in I\}$ of $\mathcal{F}_{\mathbb{C}}$ has a dual basis, and we denote the dual basis vector of b_o by λ, so that we have $\lambda(b_i) = \delta_{i,o}$. Using it, we define on $\mathcal{F}_{\mathbb{C}}$ the sesquilinear form

$$\langle x, y \rangle := \lambda(xy^*)$$

Now it follows from Proposition 1.1.3 that the basis $\{b_i \mid i \in I\}$ is orthonormal with respect to this sesquilinear form, which shows that the sesquilinear form is also positive definite, i.e., a scalar product on $\mathcal{F}_{\mathbb{C}}$. This shows in particular that $xx^* = 0$ implies $x = 0$ for all $x \in \mathcal{F}_{\mathbb{C}}$.

From Corollary 1.2.2, we see that the primitive idempotents $p_i \in \mathcal{F}_K$ are already contained in $\mathcal{F}_{\mathbb{Q}_{N_o}}$. By choosing a fixed embedding of $\mathbb{Q}_{N_o}$ into $\mathbb{C}$, we can regard them as elements of $\mathcal{F}_{\mathbb{C}}$. Because $*$ is a ring automorphism, p_i^* is again a primitive idempotent, and therefore $p_i \neq p_i^*$ implies $p_i p_i^* = 0$, which would imply $p_i = 0$ by the preceding argument. This shows that $p_i = p_i^*$ for all $i \in I$. Writing this out in the explicit form of these elements given in Corollary 1.2.2, this means that

$$\frac{1}{\xi_i(b_A)} \sum_{j \in I} \xi_i(b_{j^*}) b_j = \frac{1}{\xi_i(b_A)} \sum_{j \in I} \gamma(\xi_i(b_{j^*})) b_{j^*}$$

where we have used that $\xi_i(b_A) = \frac{n}{n_i^2}$ is a rational number by Corollary 1.2.1. This shows that $\xi_i(b_{j^*}) = \gamma(\xi_i(b_j))$. By the definition of the action of the Galois group, this means that $\xi_i(b_{j^*}) = \xi_i(\gamma.b_j)$, which implies by Proposition 1.4 that $b_{j^*} = \gamma.b_j = b_{\gamma.j}$, as asserted. $\square$

The preceding argument is adapted from [58], Sec. 2, Rem. 11, p. 1088, resp. [75], Sec. 3, Prop. 3.1, p. 885; a slightly different argument can be found in [5], § 6, Cor. 6.2, p. 88. Note that it implies in particular that $\sigma.i^* = (\sigma.i)^*$ for all automorphisms $\sigma \in \mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$, since this group is abelian.

1.6   As we said in the introduction and will see in Paragraph 4.4 in explicit example, the Gaussian sum $\mathfrak{g}$ is in general not equal to the reciprocal Gaussian sum $\mathfrak{g}'$. However, they differ only by a root of unity:

Proposition   Let m be the cardinality of I.

1. We have $\mathfrak{g}^{2Nm} = \mathfrak{g}'^{2Nm}$.

2. If the modular datum is integral, we have $\mathfrak{g}^{2N} = \mathfrak{g}'^{2N}$.

3. If the modular datum is integral and N is even, we have $\mathfrak{g}^N = \mathfrak{g}'^N$.

Proof.   (1) By taking determinants on both sides of the equation $\mathbf{S}^2 = n\mathbf{C}$, we get that
$$\det(\mathbf{S})^2 = n^m \det(\mathbf{C}) = \pm n^m$$

because $\mathbf{C}$ is a permutation matrix. Similarly, we get by taking determinants in the constant form of Axiom 1.1.4 that

$$\mathfrak{g}^m = (\frac{n_o}{t_o^2})^m \det(\mathbf{T})^3 \det(\mathbf{S})$$

18

Combining both equations and using Proposition 1.1.5, we get that

$$\mathfrak{g}^{2m} = \pm(\frac{n_o}{t_o^2})^{2m} \det(\mathbf{T})^6 n^m = \pm(\frac{\mathfrak{g}\mathfrak{g}'}{t_o^4})^m \det(\mathbf{T})^6$$

which implies that

$$(\frac{\mathfrak{g}}{\mathfrak{g}'})^m = \pm\frac{1}{t_o^{4m}} \det(\mathbf{T})^6$$

Now $\det(\mathbf{T})$ is the product of the diagonal elements t_i, and therefore an N-th root of unity. This implies that $(\mathfrak{g}/\mathfrak{g}')^{2Nm} = 1$.

(2) If the modular datum is integral, $\mathfrak{g}$ and $\mathfrak{g}'$ are contained in $\mathbb{Q}_N$ by construction. But the only roots of unity contained in $\mathbb{Q}_N$ are the N-th roots of unity and their negatives (cf. [74], Exerc. 2.3, p. 17). This shows that $(\mathfrak{g}/\mathfrak{g}')^{2N} = 1$, and also that $(\mathfrak{g}/\mathfrak{g}')^N = 1$ if N is even. $\square$

1.7 As the name suggests, modular data are closely related to the (homogeneous) modular group $\mathrm{SL}(2,\mathbb{Z})$. Recall that the modular group is generated by the two matrices

$$\mathfrak{s} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathfrak{t} := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(cf. [2], Sec. 2.2, Thm. 2.1, p. 28). It is easy to see that these matrices satisfy the relations

$$\mathfrak{s}^4 = 1 \qquad (\mathfrak{t}\mathfrak{s})^3 = \mathfrak{s}^2$$

however, it is a nontrivial result that these are defining relations for the modular group (cf. [13], § 7.2, p. 85; [24], Thm. 3.2.3.2, p. 97; [39], Thm. A.2, p. 312; [40], § II.9.1, p. 454). The connection to modular data now becomes apparent if we write Axiom 1.1.3 and the constant form of Axiom 1.1.4 in the form

$$\mathbf{S}^2 = n\mathbf{C} \qquad\qquad \frac{n_o}{t_o^2}(\mathbf{TS})^3 = \mathfrak{g}\mathbf{S}^2$$

From this, we see that the assignment

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PGL}(m, K), \ \mathfrak{s} \mapsto \mathbf{S}, \mathfrak{t} \mapsto \mathbf{T}$$

defines a projective representation of the modular group, i.e., a group homomorphism to the projective general linear group $\mathrm{PGL}(m, K) := \mathrm{GL}(m, K)/K^\times$, where m is the cardinality of I (cf. Paragraph 3.1).

As we will see in a moment, it follows from the above presentation that every projective representation of the modular group can be lifted to an ordinary representation, at least if the base field K is algebraically closed. But doing this in our case requires to rescale the Verlinde matrix and the Dehn matrix by two scalars, and as these scalars are not completely determined, certain choices can be made. We now introduce the notion of an extended modular datum for a modular datum for which these choices have been made:

Definition Suppose that K is a field of characteristic zero. An extended modular datum over K is a septuple $(I, o, {}^*, \mathbf{S}, \mathbf{T}, D, \ell)$ such that $(I, o, {}^*, \mathbf{S}, \mathbf{T})$ is a modular datum and D and ℓ are elements of K that satisfy

$$D^4 = n^2 \qquad \ell^3 = \frac{\mathfrak{g}}{n_o t_o D}$$

where n is the global dimension and $\mathfrak{g}$ is the Gaussian sum of the modular datum. The number D is called the generalized rank of the extended modular datum. A generalized rank is called a rank if $D^2 = n$. The number ℓ is called the (multiplicative) central charge of the extended modular datum. The matrices

$$\mathbf{S}' := \frac{\mathbf{S}}{D} \qquad \text{and} \qquad \mathbf{T}' := \frac{\mathbf{T}}{t_o \ell}$$

are called the homogeneous Verlinde matrix resp. the homogeneous Dehn matrix of the extended modular datum.

The notion of rank is adapted from [73], Sec. II.1.6, p. 76. If we rescale the Verlinde matrix with a rank, Axiom 1.1.3 takes the form $(\mathbf{S}/D)^2 = \mathbf{C}$. Note that it follows from Proposition 1.1.5 that, if $\mathfrak{g} = \mathfrak{g}'$, the two possible ranks are $D = \pm \mathfrak{g}/n_o$, so that the condition on the central charge becomes $\ell^3 = \pm 1/t_o$.

On the other hand, we know from Axiom 1.1.3 that the Verlinde matrix has at most four different eigenvalues, namely exactly the four possible values for a generalized rank. If we rescale the Verlinde matrix with a generalized rank, we do not always have the equation $(\mathbf{S}/D)^2 = \mathbf{C}$, but in any case we have $(\mathbf{S}/D)^4 = \mathbf{E}$, which is one of the defining relations of the modular group. If $\mathfrak{g} = \pm \mathfrak{g}'$, it follows again from Proposition 1.1.5 that $D = \mathfrak{g}/n_o$ is a possible generalized rank, and the other possibilities deviate from this one by a fourth root of unity. If $D = \mathfrak{g}/n_o$, the condition on the central charge becomes $\ell^3 = 1/t_o$.

The following observation is easy but important:

Proposition The central charge is a root of unity.

Proof. From Proposition 1.1.5, we get that

$$\ell^3 = \frac{\mathfrak{g}}{n_o t_o D} = \pm \frac{D n_o}{t_o \mathfrak{g}'}$$

which implies that $t_o^2 \ell^6 = \pm \mathfrak{g}/\mathfrak{g}'$. Now Proposition 1.6 implies the assertion. $\square$

Let us now see which role these quantities play in the lifting of the projective representation of the modular group to an ordinary linear representation. With a generalized rank D and the multiplicative central charge ℓ, we can write Axiom 1.1.3 and Axiom 1.1.4 in the form

$$\mathbf{S}^2 = \pm D^2 \mathbf{C} \qquad\qquad (\mathbf{T}\mathbf{S})^3 = D t_o^3 \ell^3 \mathbf{S}^2$$

20

which implies

$$(\frac{\mathbf{S}}{D})^4 = \mathbf{E} \qquad\qquad (\frac{\mathbf{T}}{t_o\ell}\frac{\mathbf{S}}{D})^3 = (\frac{\mathbf{S}}{D})^2$$

so that the assignment

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(m, K), \ \mathfrak{s} \mapsto \mathbf{S}' = \frac{\mathbf{S}}{D}, \mathfrak{t} \mapsto \mathbf{T}' = \frac{\mathbf{T}}{t_o\ell}$$

yields a linear representation of the modular group.

We note that extended modular data can be rescaled in the following way: If μ is a nonzero number and ζ is a root of unity, then $(I, o, {}^*, \mu\mathbf{S}, \zeta\mathbf{T}, \mu D, \ell)$ is again an extended modular datum, because the Gaussian sum corresponding to the rescaled matrices is $\mu^2\zeta\mathfrak{g}$. Clearly, the homogeneous Verlinde matrix and the homogeneous Dehn matrix are not changed by this rescaling, so that the resulting representation of the modular group is the same. We will discuss still another way of modifying extended modular data in Paragraph 2.1.

It is instructive to consider the case of an integral modular datum over the field $K = \mathbb{C}$: In this case, we have $D = \pm\sqrt{n} \in \mathbb{R}$ for a rank, and $D = \pm i\sqrt{n}$ for a generalized rank that is not a rank. It then follows from Proposition 1.5 that the homogeneous Verlinde matrix $\mathbf{S}'$ becomes unitary, a property that the Dehn matrix and the homogeneous Dehn matrix always have, as their diagonal entries are roots of unity. In this case, we can also write ℓ in the form

$$\ell = e^{2\pi ic/24}$$

for a number $c \in \mathbb{C}$, which is unique modulo $24\mathbb{Z}$. This number c is then called the additive central charge of the extended modular datum. As we saw above, ℓ is a root of unity, which means that c is in fact a rational number.

Our exposition in this paragraph follows essentially [3], Sec. 3.1, in particular Eq. (3.1.17), p. 51 and Rem. 3.1.20, p. 58 (cf. also [21], Prop. 3.4, p. 595). We note that in [68] and [73], the conventions are slightly different; essentially, the matrices $\mathbf{S}$ and $\mathbf{SC}$ are interchanged (cf. [68], Prop. 5.3, p. 48; [73], Sec. II.3.9, p. 98). A more comprehensive comparison of the notation used in some of these references can be found in the table at the end of Paragraph 4.2.

2 Odd Exponents

2.1 We have already introduced the notions of normalization and integrality for modular data, but we will need some further properties. Recall that the principal congruence subgroup of level N is the subgroup

$$\Gamma(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid a \equiv d \equiv 1, \ b \equiv c \equiv 0 \pmod{N} \}$$

of $\mathrm{SL}(2,\mathbb{Z})$; in other words, $\Gamma(N)$ is the kernel of the natural map

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}_N)$$

that reduces all entries of a matrix modulo N.

Definition
1. A modular datum is called a projective congruence datum if $\Gamma(N_o)$ is contained in the kernel of the projective representation

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PGL}(m,K), \ \mathfrak{s} \mapsto \mathbf{S}, \mathfrak{t} \mapsto \mathbf{T}$$

where N_o is the normalized exponent of the modular datum.

2. An extended modular datum is called a congruence datum if $\Gamma(N_o)$ is contained in the kernel of the (ordinary) representation

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(m,K), \ \mathfrak{s} \mapsto \mathbf{S}', \mathfrak{t} \mapsto \mathbf{T}'$$

where $\mathbf{S}'$ is the homogeneous Verlinde matrix and $\mathbf{T}'$ is the homogeneous Dehn matrix.

3. An integral modular datum is called Galois if we have

$$t_{\sigma.i} = \sigma^2(t_i)$$

for all $i \in I$ and all $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$.

The notions that we have introduced for modular data of course also apply to extended modular data, and, in this sense, a congruence datum is clearly a projective congruence datum. Furthermore, it is obvious that the property of being a projective congruence datum remains unchanged if we rescale the Verlinde and the Dehn matrix by appropriate factors, because this rescaling does not affect N_o. This also holds for the property of being a congruence datum if we rescale as indicated in Paragraph 1.7, as we noted there that the homogeneous Verlinde matrix and the homogeneous Dehn matrix remain unchanged. On the other hand, the property of being Galois is not invariant under rescaling. We also note that, by definition, every Galois modular datum is integral.

Even if it is possible to extend a projective congruence datum to a congruence datum by choosing a generalized rank D and a central charge ℓ, a different choice of these two numbers will in general not extend this projective congruence datum to a congruence datum. To understand this, let us first consider in how many ways a given modular datum can be extended:

Lemma Suppose that $(I, o, {}^*, \mathbf{S}, \mathbf{T}, D, \ell)$ is an extended modular datum.

1. If ζ is a twelfth root of unity, then $(I, o, {}^*, \mathbf{S}, \mathbf{T}, D/\zeta^3, \zeta\ell)$ is again an extended modular datum.

2. Conversely, if $(I, o, {}^*, \mathbf{S}, \mathbf{T}, \tilde{D}, \tilde{\ell})$ is an extended modular datum, then there exists a twelfth root of unity ζ such that $\tilde{D} = D/\zeta^3$ and $\tilde{\ell} = \zeta\ell$.

Proof. The first assertion follows immediately from Definition 1.7. For the second assertion, we get from the conditions $D^4 = n^2 = \tilde{D}^4$ that $D/\tilde{D}$ is a fourth root of unity, and the equations

$$\ell^3 = \frac{\mathfrak{g}}{n_o t_o D} \qquad\qquad \tilde{\ell}^3 = \frac{\mathfrak{g}}{n_o t_o \tilde{D}}$$

imply that $\tilde{\ell}^3/\ell^3 = D/\tilde{D}$, so that $\tilde{\ell}/\ell$ is a twelfth root of unity. $\square$

This lemma tells us that extensions are unique up to twelfth roots of unity. However, if D was a rank and we also want that $\tilde{D}$ is a rank, then we are limited to sixth roots of unity. And if we even want that $D = \tilde{D}$, then we can only use third roots of unity for the modification.

Returning to the original question, consider a congruence datum with generalized rank D and central charge ℓ, and introduce, as in the lemma, a new generalized rank $\tilde{D} = D/\zeta^3$ and a new central charge $\tilde{\ell} = \zeta\ell$, where ζ is a twelfth root of unity. If the new choices also lead to a congruence datum, then the two representations

$$\mathfrak{s} \mapsto \frac{\mathbf{S}}{D}, \ \mathfrak{t} \mapsto \frac{\mathbf{T}}{t_o \ell} \qquad \text{and} \qquad \mathfrak{s} \mapsto \frac{\mathbf{S}}{\tilde{D}}, \ \mathfrak{t} \mapsto \frac{\mathbf{T}}{t_o \tilde{\ell}}$$

of the modular group both factor over the reduced modular group $\mathrm{SL}(2, \mathbb{Z}_{N_o})$, which implies that the map

$$\mathrm{SL}(2, \mathbb{Z}_{N_o}) \to K^\times, \ \bar{\mathfrak{s}} \mapsto \frac{\tilde{D}}{D} = \frac{1}{\zeta^3}, \ \bar{\mathfrak{t}} \mapsto \frac{\tilde{\ell}}{\ell} = \zeta$$

defines a one-dimensional representation and therefore factors over the commutator factor group $\mathrm{SL}(2, \mathbb{Z}_{N_o})_{\mathrm{ab}}$. But this commutator factor group is cyclic, and its order is the greatest common divisor of N_o and 12 (cf. [7], Lem. (1.13), p. 25). In particular, if N_o is an odd number that is not divisible by 3, then the

commutator factor group is trivial, and we must have $\zeta = 1$, $\tilde{D} = D$, and $\tilde{\ell} = \ell$, so that our generalized rank and our central charge are uniquely determined by the congruence requirement. In Paragraph 4.4, we will see explicit examples where N_o is odd and not divisible by 3.

The following table summarizes in short form the properties of modular data that we have introduced:

Property	Definition	Paragraph
normalized	$n_o = t_o = 1$	1.1
integral	$n_i \in \mathbb{N}$	1.1
extended	D and ℓ chosen	1.7
projective congruence	$\mathrm{SL}(2, \mathbb{Z}_{N_o}) \to \mathrm{PGL}(m, K)$	2.1
congruence	$\mathrm{SL}(2, \mathbb{Z}_{N_o}) \to \mathrm{GL}(m, K)$	2.1
Galois	$t_{\sigma.i} = \sigma^2(t_i)$	2.1

2.2 Recall the classical isomorphism

$$\mathbb{Z}_N^\times \to \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}), \ \bar{q} \mapsto \sigma_q$$

between the group of units $\mathbb{Z}_N^\times$ of the ring $\mathbb{Z}_N$ and the Galois group of the cyclotomic field that maps a residue class $\bar{q}$ to the automorphism σ_q that raises every N-th root of unity to its q-th power. By analogy with the Hopf symbol introduced in [68], Par. 12.1, p. 114, we associate with every integral modular datum its fusion symbol:

Definition Consider an integral modular datum with exponent N and Gaussian sum $\mathfrak{g}$. For $q \in \mathbb{Z}$, we define the fusion symbol

$$\mathfrak{f}(q) := \begin{cases} \dfrac{\sigma_q(\mathfrak{g})}{\mathfrak{g}} & : \gcd(q, N) = 1 \\ 0 & : \gcd(q, N) \neq 1 \end{cases}$$

The fusion symbol should be viewed as a 1-cocycle in the following way (cf. [66], Chap. VII, § 3, p. 113): The Galois group $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ acts on the multiplicative group $\mathbb{Q}_N^\times$ of nonzero elements in the cyclotomic field. The element $\mathfrak{g} \in \mathbb{Q}_N^\times$ then can be viewed as a 0-cochain, and therefore gives rise to a 1-coboundary

$$\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \to \mathbb{Q}_N^\times, \ \sigma \mapsto \frac{\sigma(\mathfrak{g})}{\mathfrak{g}}$$

which is essentially the fusion symbol, as σ_q is mapped to $\mathfrak{f}(q)$. Now every 1-coboundary is in particular a 1-cocycle, and the 1-cocycle condition means for the fusion symbol that

$$\mathfrak{f}(qq') = \mathfrak{f}(q)\sigma_q(\mathfrak{f}(q'))$$

Actually, it follows from a version of Hilbert's theorem 90 that every cocycle is a coboundary in this situation (cf. [66], Chap. X, § 1, Prop. 2, p. 150). This equation also shows that the fusion symbol is a Dirichlet character, i.e., satisfies

$$\mathfrak{f}(qq') = \mathfrak{f}(q)\mathfrak{f}(q')$$

for all $q, q' \in \mathbb{Z}_N^{\times}$, if and only if $\sigma_q(\mathfrak{f}(q')) = \mathfrak{f}(q')$, i.e., if and only if $\mathfrak{f}(q')$ is invariant under the Galois group, which means that it is a rational number. In this case, we have $\mathfrak{f}(q') = \pm 1$, because $\{1, -1\}$ is the largest finite multiplicative subgroup of $\mathbb{Q}^{\times}$.

It is obvious that $\mathfrak{f}(q)$ depends only on the residue class of q modulo N, and also that $\mathfrak{f}(1) = 1$ and $\mathfrak{f}(-1) = \mathfrak{g}'/\mathfrak{g}$. Therefore, the following result generalizes Proposition 1.6:

Proposition Suppose that the modular datum is integral, and that $q \in \mathbb{Z}$ is relatively prime to N. Then we have $\mathfrak{f}(q)^{2N} = 1$. If N is even, we have $\mathfrak{f}(q)^N = 1$.

Proof. We have already seen in Paragraph 1.6 that $\det(\mathbf{S})^2 = \pm n^m$, where m is the cardinality of I. Since $\det(\mathbf{S}) \in \mathbb{Q}_N$ by Proposition 1.1.4, this equation implies that $\sigma_q(\det(\mathbf{S})) = \pm \det(\mathbf{S})$. We have also seen in Paragraph 1.6 that

$$\mathfrak{g}^m = (\frac{n_o}{t_o^2})^m \det(\mathbf{T})^3 \det(\mathbf{S})$$

Applying σ_q to this equation, we get

$$\sigma_q(\mathfrak{g})^m = \pm(\frac{n_o}{t_o^{2q}})^m \sigma_q(\det(\mathbf{T}))^3 \det(\mathbf{S})$$

If we divide the two equations by each other, we therefore get that

$$\mathfrak{f}(q)^m = \frac{\sigma_q(\mathfrak{g})^m}{\mathfrak{g}^m} = \pm(\frac{t_o^2}{t_o^{2q}})^m \frac{\sigma_q(\det(\mathbf{T}))^3}{\det(\mathbf{T})^3}$$

Since $\det(\mathbf{T})$ and t_o are N-th roots of unity, this implies that $\mathfrak{f}(q)^{2Nm} = 1$. But $\mathfrak{f}(q) \in \mathbb{Q}_N$ by definition, and if N is even, the only roots of unity contained in this cyclotomic field are the N-th roots of unity (cf. [74], Exerc. 2.3, p. 17). If N is odd, it still follows from the same argument that at least $\pm\mathfrak{f}(q)$ is an N-th root of unity, which implies the assertion. $\square$

One of our main goals in the sequel is to sharpen the preceding proposition. As a first step, we record the following consequence, continuing to assume that the modular datum is integral:

Corollary The fusion symbol is a Dirichlet character if and only if $\mathfrak{g}' = \pm\mathfrak{g}$. In this case, we have $\mathfrak{f}(q) \in \{0, 1, -1\}$ for all $q \in \mathbb{Z}$.

Proof. We have already discussed above that $\mathfrak{f}(q) \in \{0, 1, -1\}$ if the fusion symbol is a Dirichlet character, and also that in this case $\mathfrak{g}'/\mathfrak{g} = \mathfrak{f}(-1) = \pm 1$. So, suppose now that conversely $\mathfrak{g}' = \pm\mathfrak{g}$. Expressed differently, this means that $\gamma(\sum_{i \in I} n_i^2 t_i) = \pm \sum_{i \in I} n_i^2 t_i$. If q is relatively prime to N, we can apply the automorphism σ_q to this equation to get $\gamma(\sum_{i \in I} n_i^2 t_i^q) = \pm \sum_{i \in I} n_i^2 t_i^q$, where we have used that σ_q commutes with γ because the Galois group is abelian. Dividing this equation by the preceding one, we obtain $\gamma(\mathfrak{f}(q)) = \mathfrak{f}(q)$. But since $\mathfrak{f}(q)$ is a root of unity by the preceding result, we also have $\gamma(\mathfrak{f}(q)) = 1/\mathfrak{f}(q)$. Therefore $\mathfrak{f}(q)^2 = 1$ and $\mathfrak{f}(q) \in \{1, -1\}$. $\square$

2.3 Our second step to improve Proposition 2.2 is to show that, for Galois modular data, the fusion symbols are in fact twelfth roots of unity. For this, we recall the so-called 'definition of 24' (cf. [11], § 2.4, Prop. 3.b, p. 9; [12], Sec. 2.2, p. 691; [27], Sec. 2.5.1, p. 168):

Lemma Suppose that ξ is an N-th root of unity, and that $\xi^{q^2} = \xi$ for all $q \in \mathbb{Z}$ that are relatively prime to N. Then $\xi^{24} = 1$.

Proof. Recall that our base field K has characteristic zero. Choose a primitive N-th root of unity ζ in its algebraic closure and write $\xi = \zeta^k$ for some k, so that we have $\zeta^{kq^2} = \zeta^k$. This implies $kq^2 \equiv k \pmod{N}$ for all q that are relatively prime to N, which means that N divides $k(q^2 - 1)$. If N is odd, we see by taking $q = 2$ that N divides $3k$, so that $\xi^3 = \zeta^{3k} = 1$.

If N is even, and $N = \prod_i p_i^{k_i}$ is the prime factorization of N into powers of distinct primes, we can by the Chinese remainder theorem find a unit q modulo N that satisfies $q \equiv 3 \pmod{p_i^{k_i}}$ if $p_i = 2$ and $q \equiv 2 \pmod{p_i^{k_i}}$ if $p_i \neq 2$. If $p_i = 2$, we therefore get that $p_i^{k_i}$ divides $8k$, and if $p_i \neq 2$, $p_i^{k_i}$ divides $3k$. In any case, $p_i^{k_i}$ divides $24k$, so that N divides $24k$, showing that $\xi^{24} = \zeta^{24k} = 1$. $\square$

For example, this lemma implies that for Galois modular data we have $t_o^{24} = 1$, as the Galois condition and Proposition 1.4 imply $\sigma^2(t_o) = t_{\sigma.o} = t_o$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$. It can be used in a similar way to derive our improved statement:

Proposition For a Galois modular datum, we have $\mathfrak{f}(q)^{12} = 1$ for all $q \in \mathbb{Z}$ that are relatively prime to N.

Proof. (1) By possibly enlarging the base field, we can choose a rank D for the modular datum. From Proposition 1.1.5, we then have $\mathfrak{g}/n_o D = n_o D/\mathfrak{g}'$ and therefore
$$\left(\frac{\mathfrak{g}}{n_o D}\right)^2 = \frac{\mathfrak{g}}{\mathfrak{g}'}$$
so that Proposition 1.6 implies that $\mathfrak{g}/n_o D$ is a $4N$-th root of unity. Because $\mathfrak{g} \in \mathbb{Q}_N$ and $n_o \in \mathbb{Z}$, this also implies that $D \in \mathbb{Q}_{4N}$.

(2) For any $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, it follows directly from the Galois property and Proposition 1.4 that

$$\sigma^2(\mathfrak{g}) = \sum_{i \in I} n_i^2 \sigma^2(t_i) = \sum_{i \in I} n_{\sigma.i}^2 t_{\sigma.i} = \mathfrak{g}$$

Similarly, we have for $\sigma \in \mathrm{Gal}(\mathbb{Q}_{4N}/\mathbb{Q})$ that $\sigma(D)^2 = \sigma(n) = n$ and therefore $\sigma(D) = \pm D$, which implies that $\sigma^2(D) = D$. Both facts together show that $\sigma^2(\mathfrak{g}/n_o D) = \mathfrak{g}/n_o D$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_{4N}/\mathbb{Q})$. Now the lemma above implies that $(\mathfrak{g}/n_o D)^{24} = 1$.

(3) Now suppose that N is odd. Since we have already seen that $(\mathfrak{g}/n_o D)^{4N} = 1$, we then have $(\mathfrak{g}/n_o D)^{12} = 1$, as the greatest common divisor of 24 and $4N$ now divides 12. If q is relatively prime to $4N$, we can apply σ_q to this equation to get $(\sigma_q(\mathfrak{g}/n_o D))^{12} = 1$, and if we divide this equation by the preceding one, we get

$$\mathfrak{f}(q)^{12} \left(\frac{D}{\sigma_q(D)}\right)^{12} = \left(\frac{\sigma_q(\mathfrak{g})}{\mathfrak{g}}\right)^{12} \left(\frac{D}{\sigma_q(D)}\right)^{12} = 1$$

Now we saw in the preceding step that $\sigma_q(D)^2 = n = D^2$, so that our assertion $\mathfrak{f}(q)^{12} = 1$ holds if q is relatively prime to $4N$. But as $\mathfrak{f}(q)$ depends only on the residue class of q modulo N and the canonical map from $\mathbb{Z}_{4N}^\times$ to $\mathbb{Z}_N^\times$ is surjective, the assertion also holds if q is only relatively prime to N.

(4) Now suppose that N is even. If q is relatively prime to N, then q is odd and also relatively prime to $4N$. Since $\mathfrak{g}/n_o D$ is a $4N$-th root of unity, we have

$$\sigma_q\left(\frac{\mathfrak{g}}{n_o D}\right) = \left(\frac{\mathfrak{g}}{n_o D}\right)^q$$

which together with $\sigma_q(D) = \pm D$ implies that

$$\mathfrak{f}(q) = \frac{\sigma_q(\mathfrak{g})}{\mathfrak{g}} = \pm\left(\frac{\mathfrak{g}}{n_o D}\right)^{q-1}$$

Because q is odd, $q - 1$ is even and $12(q - 1)$ is divisible by 24, so that we get $\mathfrak{f}(q)^{12} = (\mathfrak{g}/n_o D)^{12(q-1)} = 1$, as asserted. $\square$

Note that this result means in particular that $\mathfrak{g}'/\mathfrak{g} = \mathfrak{f}(-1)$ is a 12-th root of unity. In the case where N is odd, the preceding result will be improved in Theorem 2.5.

The lemma above has another consequence that is worth noting: As we have seen, it follows from Proposition 1.1.4 that, for integral modular data, the entries of the Verlinde matrix are contained in the cyclotomic field $\mathbb{Q}_N$, which implies that we have a field extension

$$L := \mathbb{Q}(\{s_{ij} | i, j \in I\}) \subset \mathbb{Q}_N = \mathbb{Q}(\{t_i | i \in I\})$$

about which we can say the following:

Corollary If the modular datum is Galois, then the index $[\mathbb{Q}_N : L]$ is a power of 2. If in addition $L = \mathbb{Q}$, then $[\mathbb{Q}_N : L]$ divides 8 and N divides 24.

Proof. By the fundamental theorem of Galois theory, the index $[\mathbb{Q}_N : L]$ is equal to the order of the Galois group $\mathrm{Gal}(\mathbb{Q}_N/L)$, which is a subgroup of $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/L)$, then we have $s_{ij} = \sigma(s_{ij}) = s_{\sigma.i,j}$ by Proposition 1.4, which implies that $\sigma.i = i$ for all $i \in I$. By the Galois condition, we then have $\sigma^2(t_i) = t_{\sigma.i} = t_i$, so that $\sigma^2 = \mathrm{id}$. This shows that $\mathrm{Gal}(\mathbb{Q}_N/L)$ has exponent 2. By Cauchy's theorem, this implies that the order of $\mathrm{Gal}(\mathbb{Q}_N/L)$ is a power of 2.

If $L = \mathbb{Q}$, then this argument shows that $\sigma^2(t_i) = t_i$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, so that $t_i^{24} = 1$ by the preceding lemma, which implies that N divides 24. This in turn implies that $[\mathbb{Q}_N : \mathbb{Q}]$ divides $[\mathbb{Q}_{24} : \mathbb{Q}] = 8$. $\square$

We note that at least the second half of this corollary is present in [12], Sec. 3.3, p. 698, which also contains an example that shows that $L = \mathbb{Q}$ actually can occur.

2.4 Like every permutation, the permutation $i \mapsto \sigma.i$ that an automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}_{N_o}/\mathbb{Q})$ induces on the index set of an integral modular datum gives rise to a permutation matrix, which we denote by

$$P(\sigma) := (\delta_{i,\sigma.j})_{i,j\in I}$$

Note that $P(\gamma) = \mathbf{C}$ by Proposition 1.5, so that in particular $P(\sigma)$ commutes with $\mathbf{C}$. With the Verlinde matrix, this permutation matrix has the following commutation relation (cf. [68], Cor. 10.1, p. 97):

Lemma $\mathbf{S}P(\sigma) = P(\sigma)^{-1}\mathbf{S}$

Proof. From Proposition 1.4, we get

$$P(\sigma)^{-1}\mathbf{S} = (\sum_{k\in I} \delta_{i,\sigma^{-1}.k} s_{kj})_{i,j} = (s_{\sigma.i,j})_{i,j} = (\sigma(s_{i,j}))_{i,j} = (s_{i,\sigma.j})_{i,j} = \mathbf{S}P(\sigma)$$

as asserted. $\square$

The following argument, which is an adaption of the one found in [11], § 2.3, Thm. 2, p. 7f, shows that for Galois modular data the permutation matrix can be computed from the Verlinde matrix and the Dehn matrix:

Proposition Consider a Galois modular datum with Verlinde matrix $\mathbf{S}$ and Dehn matrix $\mathbf{T}$. Suppose that $q, q' \in \mathbb{Z}$ satisfy $qq' \equiv 1 \pmod{N}$. Then we have

$$\mathbf{S}\mathbf{T}^{q'}\mathbf{S}^{-1}\mathbf{T}^q\mathbf{S}\mathbf{T}^{q'} = \frac{t_o^{2q}}{n_o}\sigma_q(\mathfrak{g})\,P(\sigma_q^{-1})$$

Proof. In the constant form of Axiom 1.1.4, we bring all matrices to one side and write out the resulting equation $(\mathbf{ST})^3 = \frac{t_o^2}{n_o}\mathfrak{g}n\mathbf{C}$ in components. Then we get

$$\sum_{j,k\in I} s_{ij}t_j s_{jk}t_k s_{kl}t_l = \frac{t_o^2}{n_o}\mathfrak{g}n\delta_{i,l^*}$$

If we apply σ_q to this equation, it becomes

$$\sum_{j,k\in I} s_{i,\sigma_q.j}t_j^q s_{\sigma_q.j,k}t_k^q s_{k,\sigma_q.l}t_l^q = \frac{n}{n_o}t_o^{2q}\sigma_q(\mathfrak{g})\delta_{i,l^*}$$

by Proposition 1.4. If we replace j by $\sigma_q^{-1}.j$ and l by $\sigma_q^{-1}.l$, this becomes

$$\frac{n}{n_o}t_o^{2q}\sigma_q(\mathfrak{g})\delta_{i,\sigma_q^{-1}.l^*} = \sum_{j,k\in I} s_{ij}t_{\sigma_q^{-1}.j}^q s_{jk}t_k^q s_{kl}t_{\sigma_q^{-1}.l}^q = \sum_{j,k\in I} s_{ij}t_j^{q'} s_{jk}t_k^q s_{kl}t_l^{q'}$$

where in the last step we have used the Galois hypothesis. But this is the component form of the matrix equation

$$\mathbf{ST}^{q'}\mathbf{ST}^q\mathbf{ST}^{q'} = \frac{n}{n_o}t_o^{2q}\sigma_q(\mathfrak{g})\,P(\sigma_q^{-1})\mathbf{C}$$

which is equivalent to the assertion. $\square$

2.5 From the relation between the Verlinde matrix, the Dehn matrix, and the permutation matrices given in Proposition 2.4, we can derive the following relation for the matrix elements:

Proposition Consider a Galois modular datum, and suppose that q and r are relatively prime to N. Choose numbers q' and r' such that $qq' \equiv rr' \equiv 1$ (mod N). Then we have

$$\sigma_r(\mathfrak{g})\sum_{k\in I} s_{i^*,k}s_{jk}t_k^{q-r} = t_o^{2(q-r)}\sigma_q(\mathfrak{g})\,t_i^{-q'}t_j^{r'}\sum_{k\in I} s_{\sigma_{q'}.i,k^*}s_{\sigma_{r'}.j,k}t_k^{r'-q'}$$

Proof. From Proposition 2.4, it follows that

$$\mathbf{S}^{-1}\mathbf{T}^q\mathbf{S} = \frac{t_o^{2q}}{n_o}\sigma_q(\mathfrak{g})\,\mathbf{T}^{-q'}\mathbf{S}^{-1}P(\sigma_q^{-1})\mathbf{T}^{-q'}$$

Inverting this relation and substituting r for q, we get

$$\sigma_r(\mathfrak{g})\mathbf{S}^{-1}\mathbf{T}^{-r}\mathbf{S} = \frac{n_o}{t_o^{2r}}\,\mathbf{T}^{r'}P(\sigma_r)\mathbf{ST}^{r'}$$

Multiplying these two equations, we get

$$\sigma_r(\mathfrak{g})\mathbf{S}^{-1}\mathbf{T}^{q-r}\mathbf{S} = t_o^{2(q-r)}\sigma_q(\mathfrak{g})\,\mathbf{T}^{-q'}\mathbf{S}^{-1}P(\sigma_q^{-1})\mathbf{T}^{r'-q'}P(\sigma_r)\mathbf{ST}^{r'}$$

If we multiply this equation by the global dimension n and use that $n\mathbf{S}^{-1} = \mathbf{SC}$, we arrive at the assertion in matrix form. $\square$

The case $q = -1$, $r = 1$ of this proposition holds without the Galois condition:

Corollary For all $i, j \in I$, we have

$$\mathfrak{g} \sum_{k \in I} s_{i^*,k} s_{jk} t_k^{-2} = \mathfrak{g}' \frac{t_i t_j}{t_o^4} \sum_{k \in I} s_{ik} s_{jk} t_k^2$$

Proof. By squaring the constant form of Axiom 1.1.4, we get

$$\mathfrak{g}^2 (\mathbf{T}^{-1} \mathbf{S} \mathbf{T}^{-1})^2 = \frac{n_o^2}{t_o^4} (\mathbf{STS})^2 = \frac{\mathfrak{g}\mathfrak{g}'}{n t_o^4} (\mathbf{STS})^2$$

where we have used Proposition 1.1.5 for the second equality. Cancelling one Gaussian sum and using Axiom 1.1.3, this becomes

$$\mathfrak{g} \mathbf{T}^{-1} \mathbf{S} \mathbf{T}^{-2} \mathbf{S} \mathbf{T}^{-1} = \frac{\mathfrak{g}'}{t_o^4} \mathbf{STCTS}$$

Bringing the outer Dehn matrices to the right-hand side and the charge conjugation matrix to the left-hand side, this equation can be written in the equivalent form

$$\mathfrak{g} \mathbf{C} \mathbf{S} \mathbf{T}^{-2} \mathbf{S} = \frac{\mathfrak{g}'}{t_o^4} \mathbf{T} \mathbf{S} \mathbf{T}^2 \mathbf{S} \mathbf{T}$$

The assertion is the (i, j)-component of this matrix equation. □

From this, we can now take the third step to sharpen Proposition 2.2. We have considered the case of odd exponents already in the proof of Proposition 2.3. As we will see now, in this case the fusion symbol is not only a twelfth, but rather a second root of unity:

Theorem If the exponent N of an integral modular datum is odd, we have $\mathfrak{g} = \pm t_o^2 \mathfrak{g}'$. If the modular datum is in addition normalized, we have $\mathfrak{g} = \pm \mathfrak{g}'$ and $\mathfrak{f}(q) = \pm 1$ if q is relatively prime to N.

Proof. (1) By Proposition 1.6, $\mathfrak{g}'/\mathfrak{g}$ is a $2N$-th root of unity. We can therefore write it in the form $\mathfrak{g}'/\mathfrak{g} = v\zeta$, where $v \in \{1, -1\}$ and ζ is an N-th root of unity, so that $\mathfrak{g}' = v\zeta\mathfrak{g}$. Because N is odd, we can apply the Galois automorphism $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ to this formula. If we also divide by $\mathfrak{g}$, we get

$$\mathfrak{f}(-2) = \frac{\sigma_{-2}(\mathfrak{g})}{\mathfrak{g}} = \frac{1}{\mathfrak{g}} \sigma_2(\mathfrak{g}') = \frac{1}{\mathfrak{g}} v\zeta^2 \sigma_2(\mathfrak{g}) = v\zeta^2 \mathfrak{f}(2)$$

(2) On the other hand, setting $i = j = o$ in the preceding corollary, we get

$$\mathfrak{g} \sum_{k \in I} n_k^2 t_k^{-2} = \frac{\mathfrak{g}'}{t_o^2} \sum_{k \in I} n_k^2 t_k^2$$

30

If we divide by $\mathfrak{g}^2$, this formula becomes

$$\mathfrak{f}(-2) = \frac{v\zeta}{t_o^2}\mathfrak{f}(2)$$

Comparing this with the formula obtained in the first step, we see that $\zeta = 1/t_o^2$, which establishes the first assertion.

(3) For a normalized modular datum, we have $t_o = 1$ by definition, so that $\mathfrak{g} = \pm\mathfrak{g}'$. By Corollary 2.2, this implies $\mathfrak{f}(q) = \pm 1$ if q is relatively prime to N. $\square$

For an extended integral modular datum with odd exponent, the preceding theorem means for the multiplicative central charge that $\ell^{12} = 1$, because we have seen in the proof of Proposition 1.7 that $\ell^6 = \pm\mathfrak{g}/(t_o^2\mathfrak{g}')$. In the case $K = \mathbb{C}$, we have also explained in Paragraph 1.7 that we can write $\ell = e^{2\pi i c/24}$, where c is the additive central charge. The equation $\ell^{12} = 1$ then means that c must be an even integer. In Paragraph 5.6, we will see in an explicit example that the assumption that the exponent is odd cannot be omitted.

2.6 So far, it has not been necessary to consider classical Gaussian sums, and it is not yet apparent from our considerations why the quantity $\mathfrak{g}$ is called the Gaussian sum of the modular datum. We will explain this in Paragraph 4.4; however, as we will see now, a comparison between the Gaussian sum of a modular datum and the classical Gaussian sum leads to important new insights. Recall the definition of the classical Gaussian sum (cf. [51], Chap. V, Sec. 53, p. 177):

Definition For a primitive n-th root of unity $\zeta \in K$, the classical Gaussian sum $\mathfrak{G}$ is defined as

$$\mathfrak{G} = \mathfrak{G}_n(\zeta) := \sum_{i=0}^{n-1} \zeta^{i^2}$$

We also define $\mathfrak{G}' = \mathfrak{G}_n(1/\zeta)$.

The basic facts about classical Gaussian sums are summarized in the following nontrivial lemma, which is mainly due to C. F. Gauß (cf. [28]):

Lemma If $\iota \in K$ is a primitive fourth root of unity, we have

$$\mathfrak{G}^2 = \begin{cases} \pm 2\iota n & : n \equiv 0 \pmod 4 \\ n & : n \equiv 1 \pmod 4 \\ 0 & : n \equiv 2 \pmod 4 \\ -n & : n \equiv 3 \pmod 4 \end{cases}$$

If n is odd and q is relatively prime to n, we have

$$\sigma_q(\mathfrak{G}) = \mathfrak{G}_n(\zeta^q) = \left(\frac{q}{n}\right)\mathfrak{G}$$

where $\left(\frac{q}{n}\right)$ is the Jacobi symbol.

Proof. The first statement is proved in [51], Chap. V, Sec. 53, Thm. 99, p. 177, see also [6], Sec. 1.2, Cor. 1.2.3, p. 15 and [41], Chap. IV.VI, Thm. 211, p. 197. The second statement is proved in [59], Chap. 11, Thm. 38, p. 93, see also [6], Sec. 1.5, Thm. 1.5.2, p. 26 and [51], Chap. V, Exerc. 122, p. 187. $\square$

Under any embedding of the cyclotomic field $\mathbb{Q}_n \subset K$ into the complex numbers $\mathbb{C}$, $\mathfrak{G}'$ becomes the complex conjugate of $\mathfrak{G}$, and therefore $\mathfrak{G}\mathfrak{G}'$ becomes the square of the absolute value of $\mathfrak{G}$. Using this, we get from the lemma that

$$\mathfrak{G}\mathfrak{G}' = \begin{cases} 2n & : n \equiv 0 \pmod 4 \\ 0 & : n \equiv 2 \pmod 4 \\ n & : n \equiv 1 \text{ or } 3 \pmod 4 \end{cases}$$

In the case where also n is odd, we can use these classical results to relate the fusion symbol to the Jacobi symbol:

Theorem Suppose that both the exponent N and the global dimension n of an integral modular datum are odd. Then we have

$$t_o^2\mathfrak{g}' = (-1)^{\frac{n-1}{2}}\mathfrak{g} = \begin{cases} \mathfrak{g} & : n \equiv 1 \pmod 4 \\ -\mathfrak{g} & : n \equiv 3 \pmod 4 \end{cases}$$

If the modular datum is in addition normalized, we have $\mathfrak{f}(q) = \left(\frac{q}{n}\right)$ for all $q \in \mathbb{Z}$ that are relatively prime to Nn.

Proof. We can assume that K is algebraically closed, so that we can choose a primitive n-th root of unity ζ to form the classical Gaussian sum $\mathfrak{G} = \mathfrak{G}_n(\zeta)$. From Theorem 2.5, we know that there is a sign $v \in \{1, -1\}$ such that $\mathfrak{g} = vt_o^2\mathfrak{g}'$. Furthermore, we have $\mathfrak{g}\mathfrak{g}' = nn_o^2$ by Proposition 1.1.5, and therefore

$$\left(\frac{\mathfrak{g}}{t_o n_o}\right)^2 = \frac{v\mathfrak{g}\mathfrak{g}'}{n_o^2} = vn$$

If $v \neq (-1)^{\frac{n-1}{2}}$, i.e., $v = -(-1)^{\frac{n-1}{2}}$, we have by the preceding lemma that $\mathfrak{G}^2 = (-1)^{\frac{n-1}{2}}n = -vn$ and therefore

$$\left(\frac{\mathfrak{g}}{t_o n_o \mathfrak{G}}\right)^2 = -1$$

32

showing that $\mathfrak{g}/(t_o n_o \mathfrak{G})$ is a primitive fourth root of unity. But as we have $\mathfrak{g}/(t_o n_o) \in \mathbb{Q}_N$ and $\mathfrak{G} \in \mathbb{Q}_n$ by construction, we also have $\mathfrak{g}/(t_o n_o \mathfrak{G}) \in \mathbb{Q}_{Nn}$. As Nn is odd, this implies by [74], Exerc. 2.3, p. 17 that

$$1 = (\frac{\mathfrak{g}}{t_o n_o \mathfrak{G}})^{2Nn} = (-1)^{Nn} = -1$$

a contradiction. We therefore must have $v = (-1)^{\frac{n-1}{2}}$, which on the one hand proves the first assertion, on the other hand shows that $(\frac{\mathfrak{g}}{t_o n_o})^2 = \mathfrak{G}^2$, in other words, that $\mathfrak{g}/(t_o n_o) = \pm \mathfrak{G}$.

If the modular datum is in addition normalized, this means that $\mathfrak{g}' = (-1)^{\frac{n-1}{2}} \mathfrak{g}$ and $\mathfrak{g} = \pm \mathfrak{G}$. If q is relatively prime to Nn, this implies that

$$\mathfrak{f}(q)\mathfrak{g} = \sigma_q(\mathfrak{g}) = \pm \sigma_q(\mathfrak{G}) = \pm \left(\frac{q}{n}\right) \mathfrak{G} = \left(\frac{q}{n}\right) \mathfrak{g}$$

where the first equation holds by the definition of the fusion symbol and the third by the preceding lemma. This proves the second assertion. $\square$

The conclusion of this theorem cannot be reformulated in terms of the central charge without the assumption that the generalized rank is actually a rank. So, suppose that we extend the modular datum considered in the preceding theorem by choosing a rank D and a multiplicative central charge ℓ. We then get directly from Definition 1.7 and Proposition 1.1.5 that

$$\ell^6 = (\frac{\mathfrak{g}}{n_o t_o D})^2 = (-1)^{\frac{n-1}{2}} \frac{\mathfrak{g}\mathfrak{g}'}{n_o^2 n} = (-1)^{\frac{n-1}{2}}$$

In the case $K = \mathbb{C}$, we write, as explained in Paragraph 1.7, $\ell = e^{2\pi i c/24}$, and then find the condition

$$c \equiv 0 \pmod{4} \quad \text{if} \quad n \equiv 1 \pmod{4}$$
$$c \equiv 2 \pmod{4} \quad \text{if} \quad n \equiv 3 \pmod{4}$$

for the additive central charge c.

The hypothesis of this theorem raises the question how the prime factors of n and N are related. We will consider this question again in Paragraph 3.5.

3 Even Exponents

3.1 We will need some facts from group cohomology. Suppose that G is a finite group and that K is an algebraically closed field of characteristic zero. Recall that we have already encountered 1-cocycles in Paragraph 2.2. A 2-cocycle of G with values in the multiplicative group $K^\times$, endowed with the trivial G-action, is a function $\omega : G \times G \to K^\times$ that satisfies

$$\omega(g, g'g'')\omega(g', g'') = \omega(gg', g'')\omega(g, g')$$

for all $g, g', g'' \in G$. The set $Z^2(G, K^\times)$ of all 2-cocycles is a group under point-wise multiplication. For any map $\nu : G \to K^\times$, the equation

$$\omega(g, g') := \frac{\nu(g)\nu(g')}{\nu(gg')}$$

defines a 2-cocycle; 2-cocycles of this form are called 2-coboundaries and form a subgroup that is denoted by $B^2(G, K^\times)$. The quotient group $H^2(G, K^\times) := Z^2(G, K^\times)/B^2(G, K^\times)$ is called the second cohomology group of G with coefficients in $K^\times$, or the Schur multiplicator of G. This group is obviously abelian; it can be shown that it is also finite (cf. [31], Kap. V, Hilfssatz 23.2, p. 629). Moreover, the Schur multiplicators arising from different fields are isomorphic, as long as these fields satisfy our hypotheses above (cf. [31], Kap. V, Hauptsatz 23.5, p. 631).

The Schur multiplicator is closely related to projective representations, as explained in [31], Kap. V, § 24, p. 638ff. We will need a slight refinement of the discussion there. As usual, we embed the multiplicative group $K^\times$ of the base field into $\mathrm{GL}(m, K)$ by mapping every nonzero number to the corresponding multiple of the identity matrix. The corresponding factor group $\mathrm{PGL}(m, K) := \mathrm{GL}(m, K)/K^\times$ is called the projective linear group. Similarly, if $K_l^\times$ denotes the subgroup of $K^\times$ consisting of the l-th roots of unity, we denote the corresponding factor group by $\mathrm{P}_l\,\mathrm{GL}(m, K) := \mathrm{GL}(m, K)/K_l^\times$, so that we have a canonical group homomorphism from $\mathrm{P}_l\,\mathrm{GL}(m, K)$ to $\mathrm{PGL}(m, K)$. The exponent of the Schur multiplicator now determines how far we can lift a projective representation:

Proposition Suppose that $\alpha : G \to \mathrm{PGL}(m, K)$ is a group homomorphism, and let l be the exponent of the Schur multiplicator of G. Then there exists a group homomorphism $\beta : G \to \mathrm{P}_l\,\mathrm{GL}(m, K)$ such that the diagram

is commutative.

Proof. This follows from a minor modification of a standard argument in the theory of projective representations (cf. [31], Kap. V, Hilfssatz 23.2, p. 629): For an invertible matrix $A \in \mathrm{GL}(m, K)$, we denote its coset in $\mathrm{PGL}(m, K)$ by $AK^{\times}$ and its coset in $\mathrm{P}_l\,\mathrm{GL}(m, K)$ by $AK_l^{\times}$. For every $g \in G$, we choose a representative $A(g) \in \mathrm{GL}(m, K)$ such that $\alpha(g) = A(g)K^{\times}$. Because α is a group homomorphism, the matrix $A(g)A(g')A(gg')^{-1}$ is proportional to the unit matrix. The corresponding proportionality factor $\omega(g, g')$ is a 2-cocycle (cf. [31], Kap. V, Hilfssatz 24.2, p. 638). By assumption, $\omega(g, g')^l$ is a coboundary, so there exists a 1-cochain ν such that

$$\omega(g, g')^l = \frac{\nu(g)\nu(g')}{\nu(gg')}$$

Because K is algebraically closed, we can choose for every $g \in G$ a number $\kappa(g) \in K^{\times}$ such that $\nu(g) = \kappa(g)^l$. Then $\omega(g, g')$ and $\kappa(g)\kappa(g')/\kappa(gg')$ differ only by an l-th root of unity, which implies that

$$A(g)A(g') \qquad \text{and} \qquad \frac{\kappa(g)\kappa(g')}{\kappa(gg')}A(gg')$$

are contained in the same coset of $K_l^{\times} \subset \mathrm{GL}(m, K)$. In other words, if we define $B(g) := \frac{1}{\kappa(g)}A(g)$, then the map $\beta(g) := B(g)K_l^{\times}$ satisfies our requirements. □

We are here interested in the case where the finite group G is the reduced modular group $\mathrm{SL}(2, \mathbb{Z}_N)$. Its Schur multiplicator has been determined by F. R. Beyl (cf. [7], Thm. (3.9), p. 32):

Theorem (F. R. Beyl)

$$H^2(\mathrm{SL}(2, \mathbb{Z}_N), K^{\times}) \cong \begin{cases} \mathbb{Z}_2 & : 4 \mid N \\ \{0\} & : 4 \nmid N \end{cases}$$

If we combine this theorem with the preceding proposition, we get the following corollary, in which we have formulated the conclusion in a slightly different way:

Corollary Suppose that $\alpha : \mathrm{SL}(2, \mathbb{Z}_N) \to \mathrm{PGL}(m, K)$ is a group homomorphism. Then we can choose, for every $g \in \mathrm{SL}(2, \mathbb{Z}_N)$, a representative $A(g)$ of the coset $\alpha(g)$ in such a way that

$$A(g)A(g') = \pm A(gg')$$

for all $g, g' \in \mathrm{SL}(2, \mathbb{Z}_N)$.

Proof. As the theorem shows, the exponent l of the Schur multiplicator divides 2. As we have $K_2^{\times} = \{1, -1\}$, this implies the assertion. □

3.2   To proceed, we need to discuss certain elements of the modular group. Recall the generators $\mathfrak{s}$ and $\mathfrak{t}$ of the modular group from Paragraph 1.7. We now introduce the following matrices (cf. [25], § 1, Eq. (6), p. 230), which implicitly appear already in Proposition 2.4:

Definition   For $q, r \in \mathbb{Z}$, we define $\mathfrak{d}(q, r) := \mathfrak{s}\mathfrak{t}^r\mathfrak{s}^{-1}\mathfrak{t}^q\mathfrak{s}\mathfrak{t}^r$.

Explicitly, these matrices are

$$
\mathfrak{d}(q, r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}
$$

$$
= \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -q \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}
$$

$$
= \begin{pmatrix} 1 & q \\ -r & 1 - qr \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix} = \begin{pmatrix} q & qr - 1 \\ 1 - qr & r(2 - qr) \end{pmatrix}
$$

From this we see that, if $qr \equiv 1 \pmod{N}$, then the image of $\mathfrak{d}(q, r)$ in $\mathrm{SL}(2, \mathbb{Z}_N)$ under reduction modulo N becomes diagonal. In any case, we will denote the image of $\mathfrak{d}(q, r)$ under reduction modulo N by $\bar{\mathfrak{d}}(q, r)$.

Denoting the transpose of a 2×2-matrix A by A^T, we have the following lemma, which appears in [7], Sec. 1, no. (1.5), p. 24:

Lemma   For all $g \in \mathrm{SL}(2, \mathbb{Z})$, we have $\mathfrak{s}g^{-1} = g^T\mathfrak{s}$.

Proof.   The assertion can be reformulated by saying that the two group automorphisms $g \mapsto \mathfrak{s}g\mathfrak{s}^{-1}$ and $g \mapsto g^{-1T}$ are equal, a fact that can be verified on generators. For $g = \mathfrak{s}$, this is obvious, and for $g = \mathfrak{t}$, the corresponding calculation can be found in [68], Par. 1.1, p. 10. It is also easy to check the assertion directly. $\square$

For the matrices $\mathfrak{d}(q, r)$, this lemma implies the following commutation relations:

Proposition $\mathfrak{s}\mathfrak{d}(q, r)^{-1} = \mathfrak{d}(-q, -r)\mathfrak{s}^{-1} = \mathfrak{d}(q, r)^T\mathfrak{s}$

Proof.   For the first identity, we have

$$
\mathfrak{s}\mathfrak{d}(q, r)^{-1} = \mathfrak{s}\mathfrak{t}^{-r}\mathfrak{s}^{-1}\mathfrak{t}^{-q}\mathfrak{s}\mathfrak{t}^{-r}\mathfrak{s}^{-1} = \mathfrak{d}(-q, -r)\mathfrak{s}^{-1}
$$

The second identity follows from the preceding lemma. $\square$

Because the transpose of a diagonal matrix is equal to itself, this proposition implies in particular that $\mathfrak{s}\mathfrak{d}(q, r)^{-1} \equiv \mathfrak{d}(q, r)\mathfrak{s} \pmod{\Gamma(N)}$ if $qr \equiv 1 \pmod{N}$.

3.3 We now consider a projective congruence datum over an algebraically closed field K of characteristic zero. As explained in Paragraph 1.1, we denote its exponent by N and its normalized exponent by N_o. We then have a group homomorphism $\alpha : \mathrm{SL}(2, \mathbb{Z}_{N_o}) \to \mathrm{PGL}(m, K)$ that maps the reduced matrices $\bar{\mathfrak{s}}$ and $\bar{\mathfrak{t}}$ to the cosets of $\mathbf{S}$ resp. $\mathbf{T}$. As we saw in Paragraph 3.1, we can lift α to a group homomorphism $\beta : \mathrm{SL}(2, \mathbb{Z}_{N_o}) \to \mathrm{P}_2\, \mathrm{GL}(m, K)$. We choose two representatives $\mathbf{S}'', \mathbf{T}'' \in \mathrm{GL}(m, K)$ for the images of the generators, so that we have

$$\beta(\bar{\mathfrak{s}}) = \{\pm \mathbf{S}''\} \qquad\qquad \beta(\bar{\mathfrak{t}}) = \{\pm \mathbf{T}''\}$$

Because β lifts α, there are nonzero numbers $s, t \in K^\times$ such that

$$\mathbf{S}'' = \frac{1}{s}\mathbf{S} \qquad\qquad \mathbf{T}'' = \frac{1}{t}\mathbf{T}$$

Applying β to the defining relations of the modular group described in Paragraph 1.7, we get $\beta(\bar{\mathfrak{s}})^4 = 1$ and $(\beta(\bar{\mathfrak{t}})\beta(\bar{\mathfrak{s}}))^3 = \beta(\bar{\mathfrak{s}})^2$. Therefore, there are signs $v_s, v_t \in \{1, -1\}$ such that

$$\mathbf{S}''^4 = v_s \mathbf{E} \qquad (\mathbf{T}''\mathbf{S}'')^3 = v_t \mathbf{S}''^2$$

In terms of the parameters s and t, this equation can be written as

$$\mathbf{S}^4 = v_s s^4 \mathbf{E} \qquad (\mathbf{TS})^3 = v_t s t^3 \mathbf{S}^2$$

In Paragraph 1.7, we have rewritten part of the definition of a modular datum in the form $\mathbf{S}^2 = n\mathbf{C}$ resp. $\frac{n_o}{t_o^2}(\mathbf{TS})^3 = \mathfrak{g}\mathbf{S}^2$. Comparing this with the preceding equations, we get

$$v_s s^4 = n^2 \qquad\qquad v_t s t^3 = \frac{t_o^2}{n_o}\mathfrak{g}$$

From this, we see that the new parameters s and t are essentially roots of unity:

Proposition For an extended projective congruence datum that is also Galois, we have that s/D is an eighth root of unity and that t is a 72th root of unity, where D is the generalized rank of the extended modular datum. Moreover, for the central charge ℓ of the datum, we have

$$t^3 = v_t \frac{D}{s}t_o^3 \ell^3$$

Proof. From the first equation above, we get $s^4 = v_s n^2 = v_s D^4$, so that $(s/D)^4 = v_s$ and thus $(s/D)^8 = 1$. Dividing the second equation above by D, we get

$$v_t \frac{s}{D}t^3 = \frac{t_o^2}{n_o}\frac{\mathfrak{g}}{D} = t_o^3 \ell^3$$

where the second equation uses Definition 1.7. Squaring this and using the proof of Proposition 1.7, we get

$$\left(\frac{s}{D}\right)^2 t^6 = \pm t_o^4 \frac{\mathfrak{g}}{\mathfrak{g}'}$$

37

Now $\mathfrak{g}/\mathfrak{g}'$ is a twelfth root of unity by Proposition 2.3, and we have also discussed there that $t_o^{24} = 1$. Combining all this, we get

$$t^{72} = (\pm t_o^4 \frac{\mathfrak{g}}{\mathfrak{g}'})^{12} = 1$$

as asserted. $\square$

From this proposition, we see that the matrices $\mathbf{S}''$ and $\mathbf{T}''$ differ from the homogeneous matrices $\mathbf{S}'$ and $\mathbf{T}'$ introduced in Definition 1.7 only by roots of unity: $\mathbf{S}'$ and $\mathbf{S}''$ differ by the eighth root of unity s/D, and $\mathbf{T}'$ and $\mathbf{T}''$ differ by the 24th root of unity $t/(t_o\ell)$. While the matrices $\mathbf{S}'$ and $\mathbf{T}'$ lead to an ordinary representation of the modular group, the matrices $\mathbf{S}''$ and $\mathbf{T}''$ only lead to a representation modulo signs, but this latter homomorphism to $P_2\,GL(m, K)$ has the advantage to factor over the reduced modular group $SL(2, \mathbb{Z}_{N_o})$.

3.4 In the last paragraph, we have associated with a projective congruence datum over an algebraically closed field K of characteristic zero the group homomorphism $\beta : SL(2, \mathbb{Z}_{N_o}) \to P_2\,GL(m, K)$, the matrices $\mathbf{S}''$ and $\mathbf{T}''$, and the numbers s and t. For these quantities, we have the following analogue of Proposition 2.4:

Proposition Consider an extended projective congruence datum that is also Galois, and suppose that we are given two integers $q, q' \in \mathbb{Z}$ satisfying $qq' \equiv 1 \pmod{72N}$. Then we have

$$\beta(\bar{\mathfrak{d}}(q, q')) = \{\pm(\frac{s}{D})^{q-1} t^{2(q-q')}\,P(\sigma_q^{-1})\}$$

where D is the generalized rank of the extended modular datum.

Proof. Dividing the equation in Proposition 2.4 by $t^{2q'+q}s$, we get

$$\mathbf{S}''\mathbf{T}''^{q'}\mathbf{S}''^{-1}\mathbf{T}''^{q}\mathbf{S}''\mathbf{T}''^{q'} = \frac{t_o^{2q}}{n_o}\frac{\sigma_q(\mathfrak{g})}{t^{2q'+q}s}\,P(\sigma_q^{-1})$$

A slight modification of the argument given in the proof of Proposition 2.3 shows that $D \in \mathbb{Q}_{4N}$, so that $\sigma_q(D)$ is well-defined. Now determine $v \in \{1, -1\}$ such that $\sigma_q(D) = vD$. Using Proposition 3.3 and the formulas stated before it, we get

$$\frac{t_o^{2q}}{n_o}\sigma_q(\mathfrak{g}) = \sigma_q(\frac{t_o^2}{n_o}\mathfrak{g}) = \sigma_q(v_t D \frac{s}{D} t^3) = v_t v D(\frac{s}{D})^q t^{3q}$$

Inserting this into the preceding equation, it becomes

$$\mathbf{S}''\mathbf{T}''^{q'}\mathbf{S}''^{-1}\mathbf{T}''^{q}\mathbf{S}''\mathbf{T}''^{q'} = v_t v(\frac{s}{D})^{q-1} t^{2(q-q')}\,P(\sigma_q^{-1})$$

But according to Definition 3.2, this is what we have to verify. $\square$

This enables us to take the fourth step in the sharpening of Proposition 2.2:

Theorem For an extended projective congruence datum that is also Galois, we have $\ell^{24} = 1$ and $\mathfrak{g}^4 = t_o^8 \mathfrak{g}'^4$.

Proof. As these identities clearly still hold if we enlarge the base field, we can assume that K is algebraically closed, so that the preceding discussion applies. Recall from the proof of Proposition 1.7 that $t_o^2 \ell^6 = \pm \mathfrak{g}/\mathfrak{g}'$, so that our two assertions are equivalent. Moreover, we can assume that N is even, because otherwise we have already $\mathfrak{g} = \pm t_o^2 \mathfrak{g}'$ by Theorem 2.5.

We claim that we can also assume that N is divisible by 3: From Proposition 2.3, we know that $(\mathfrak{g}'/\mathfrak{g})^{12} = \mathfrak{f}(-1)^{12} = 1$, and we also discussed there that $t_o^{24} = 1$. Furthermore, we have $(\mathfrak{g}'/\mathfrak{g})^N = 1$ by Proposition 1.6, and $t_o^N = 1$ by definition. If N is not divisible by 3, then these equations imply together that $(\mathfrak{g}'/\mathfrak{g})^4 = 1$ and $t_o^8 = 1$, in which case our assertions hold.

In the remaining cases, N and $72N$ therefore have the same prime divisors, so that, if q is relatively prime to N, we can choose $q' \in \mathbb{Z}$ such that $qq' \equiv 1$ (mod $72N$). Since N_o divides N, we then also have $qq' \equiv 1$ (mod N_o), so that by Proposition 3.2 the matrices $\mathfrak{d}(-q, -q')$ and $\mathfrak{d}(q, q')\mathfrak{s}^2$ reduce in $\mathrm{SL}(2, \mathbb{Z}_{N_o})$ to the same diagonal matrix. We have $\beta(\bar{\mathfrak{s}}) = \{\pm \mathbf{S}''\} = \{\pm \frac{1}{s} \mathbf{S}\}$, therefore $\beta(\bar{\mathfrak{s}}^2) = \{\pm \frac{1}{s^2} \mathbf{S}^2\} = \{\pm \frac{n}{s^2} \mathbf{C}\}$, and so the preceding proposition yields

$$\{\pm (\frac{s}{D})^{-q-1} t^{2(q'-q)} P(\sigma_{-q}^{-1})\} = \beta(\bar{\mathfrak{d}}(-q, -q'))$$
$$= \beta(\bar{\mathfrak{d}}(q, q')\bar{\mathfrak{s}}^2) = \{\pm (\frac{s}{D})^{q-1} t^{2(q-q')} \frac{n}{s^2} P(\sigma_q^{-1})\mathbf{C}\}$$

Since $P(\sigma_{-1}) = P(\gamma) = \mathbf{C}$, we have $P(\sigma_{-q}^{-1}) = P(\sigma_q^{-1})\mathbf{C}$. As we have $D^2 = \pm n$, this implies that there is a sign $v \in \{1, -1\}$ such that

$$(\frac{s}{D})^{-q-1} t^{2(q'-q)} = v(\frac{s}{D})^{q-1} t^{2(q-q')} \frac{D^2}{s^2} = v(\frac{s}{D})^{q-3} t^{2(q-q')}$$

or alternatively $t^{4(q-q')} = v(\frac{s}{D})^{-2q+2}$. Now we know from Proposition 3.3 that s/D is an eighth root of unity, so that by raising the last equation to the fourth power we get $t^{16(q-q')} = 1$. The same proposition yields that $t^{72} = 1$, which means that already $t^{8(q-q')} = 1$. Raising this equation to the q-th power, it becomes $t^{8(q^2-1)} = 1$, or $t^{8q^2} = t^8$.

All of this shows that t^8 is a $72N$-th root of unity which is invariant under σ_q^2 for every q that is relatively prime to $72N$. So the 'definition of 24', given in Lemma 2.3, implies that $(t^8)^{24} = 1$. As we also have $t^{72} = (t^8)^9 = 1$, and $3 = \gcd(24, 9)$, we get $t^{24} = (t^8)^3 = 1$. Using Proposition 3.3 once again, we see that $t^3 = v_t \frac{D}{s} t_o^3 \ell^3$ is an eighth root of unity, and as $\frac{s}{D}$ and t_o^3 are also eighth roots of unity, ℓ^3 must be an eighth root of unity, too, which is the assertion. $\square$

If the modular datum is in addition normalized, the theorem obviously yields that $\mathfrak{g}^4 = \mathfrak{g}'^4$. Furthermore, we have explained in Paragraph 1.7 that in the case $K = \mathbb{C}$ we can write $\ell = e^{2\pi i c/24}$ by using the additive central charge c. The equation $\ell^{24} = 1$ then means that c must be an integer.

We note that in [11], A. Coste and T. Gannon deduce the same result from a slightly different hypothesis (cf. [11], § 2.4, Prop. 3.b, p. 9). To understand the relation of the two results, let us consider a normalized modular datum. We can extend it by choosing a generalized rank D and a multiplicative central charge ℓ, and then form the homogeneous matrices $\mathbf{S}' = \mathbf{S}/D$ and $\mathbf{T}' = \mathbf{T}/\ell$. Following their treatment in this situation, we would then assume that $\mathbf{T}'$, and not $\mathbf{T}$, satisfies the Galois condition. As the (o, o)-component of $\mathbf{T}'$ is $1/\ell$, the fact that $\ell^{24} = 1$ then follows as in our remark after Lemma 2.3; in fact, our argument there was directly adapted from the argument of Coste and Gannon. However, if we impose the Galois condition on $\mathbf{T}$ instead of $\mathbf{T}'$, then $\mathbf{T}'$ will also satisfy the Galois condition if and only if $\ell^{24} = 1$, so that the argument given by Coste and Gannon becomes unavailable. But for the applications to semisimple Hopf algebras that we have in mind, it is the Galois condition on $\mathbf{T}$ that is needed.

We conclude this paragraph with a brief table that summarizes the main results that we have obtained in short form:

Result	Assumptions	Paragraph
$\mathfrak{g}^{2N} = \mathfrak{g}'^{2N}$, $t_o^N = 1$	integral modular datum	1.6 (cf. 2.2)
$\mathfrak{g}^{12} = \mathfrak{g}'^{12}$, $t_o^{24} = 1$	Galois modular datum	2.3
$\mathfrak{g}^2 = t_o^4 \mathfrak{g}'^2$	integral modular datum, N odd	2.5
$\mathfrak{g} = (-1)^{\frac{n-1}{2}} t_o^2 \mathfrak{g}'$	integral modular datum, N and n odd	2.6
$\mathfrak{g}^4 = t_o^8 \mathfrak{g}'^4$	Galois projective congruence datum	3.4

3.5   As we already mentioned there, the hypothesis of Theorem 2.6 raises the question how the prime factors of n and N are related. As we will explain in Paragraph 4.2, every semisimple factorizable Hopf algebra leads to a modular datum whose global dimension is just the dimension of the Hopf algebra. In this situation, Cauchy's theorem for Hopf algebras (cf. [37], Thm. 3.4, p. 26) asserts that a prime that divides n also divides N. For integral modular data, we have the following weak version of this result:

Proposition   For an integral modular datum, suppose that an odd prime p divides n an odd number of times. Then it also divides N.

Proof.   Let l be the product of all primes that appear an odd number of times in the prime factorization of n. Then l is squarefree, and in the factorization

of n/l, each prime appears an even number of times, so that we can write it as a complete square $n/l = k^2$ for some positive integer k. Our assumption now means that p divides l, so that in particular $l \neq 1$.

By possibly enlarging the base field, we can choose a rank for the modular datum, i.e., a number $D \in K$ such that $D^2 = n$. Recall from the first step in the proof of Proposition 2.3 that $D \in \mathbb{Q}_{4N}$, so that the cyclotomic field $\mathbb{Q}_{4N}$ contains the quadratic number field $\mathbb{Q}(D)$, which is clearly isomorphic to the quadratic number field $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{l}) \subset \mathbb{C}$ and therefore has discriminant $4l$ if $l \equiv 2 \pmod 4$ or $l \equiv 3 \pmod 4$, and discriminant l if $l \equiv 1 \pmod 4$ (cf. [53], Kap. I, § 2, Aufg. 4, p. 16). In any case, its discriminant is divisible by p.

By the discriminant tower theorem (cf. [53], Kap. III, § 2, Kor. (2.10), p. 213), the discriminant of $\mathbb{Q}(D)$ divides the discriminant of $\mathbb{Q}_{4N}$. But a prime that divides the discriminant of $\mathbb{Q}_{4N}$ also divides $4N$ (cf. [74], Chap. 2, Prop. 2.7, p. 12; see also [53], Kap. I, § 10, Lem. (10.1), p. 62). Therefore, p divides $4N$, and therefore N. □

It is also possible to say something about the prime $p = 2$:

Corollary Consider a projective congruence datum that is also Galois. If N denotes its exponent and n its global dimension, then we have $N \equiv 0 \pmod 4$ if $n \equiv 2 \pmod 4$.

Proof. We can assume that the base field K is algebraically closed, and therefore extend the datum by choosing a generalized rank D and a central charge ℓ. We then know from Theorem 3.4 that $t_o^8 \mathfrak{g}'^4 = \mathfrak{g}^4$, and therefore $t_o^4 \mathfrak{g}'^2 = \pm \mathfrak{g}^2$. If $t_o^4 \mathfrak{g}'^2 = -\mathfrak{g}^2$, then $\mathbb{Q}_N$ contains the primitive fourth root of unity $t_o^2 \mathfrak{g}'/\mathfrak{g}$. If now N were odd, we would have $1 = (t_o^2 \mathfrak{g}'/\mathfrak{g})^{2N} = (-1)^N = -1$ by [74], Exerc. 2.3, p. 17, so N must be even. But this implies the stronger equation $(t_o^2 \mathfrak{g}'/\mathfrak{g})^N = 1$, which shows that N is divisible by 4.

We can therefore assume that $t_o^4 \mathfrak{g}'^2 = \mathfrak{g}^2$, so that $t_o^2 \mathfrak{g}' = v\mathfrak{g}$ for a sign $v \in \{1, -1\}$. According to Proposition 1.1.5, this means that $\mathfrak{g}^2 = vt_o^2 \mathfrak{g}\mathfrak{g}' = vt_o^2 nn_o^2$. As in the proof of the preceding proposition, we write $n = k^2 l$, where l is squarefree. The last equation then implies that $(\mathfrak{g}/(t_o n_o k))^2 = vl$.

Because $n \equiv 2 \pmod 4$, we must have $l = 2l'$ for an odd integer l', and l' divides N by the preceding proposition. If we denote the classical Gaussian sum coming from a primitive l'-th root of unity by $\mathfrak{G}$, then we know from Lemma 2.6 that $\mathfrak{G}^2 = (-1)^{\frac{l'-1}{2}} l'$; moreover, we have $\mathfrak{G} \in \mathbb{Q}_{l'} \subset \mathbb{Q}_N$. Combining this with the previous equation, we get

$$\left(\frac{\mathfrak{g}}{t_o n_o k \mathfrak{G}}\right)^2 = (-1)^{\frac{l'-1}{2}} \frac{vl}{l'} = \pm 2$$

On the other hand, consider a primitive eighth root of unity $\xi \in K$. Then we have $\xi^4 = -1$ and therefore

$$(\frac{1+\xi^2}{\xi})^2 = 2 \qquad \text{and} \qquad (\frac{1-\xi^2}{\xi})^2 = -2$$

This shows that

$$\frac{\mathfrak{g}}{t_o n_o k \mathfrak{G}} = \pm\frac{1+\xi^2}{\xi} \qquad \text{or} \qquad \frac{\mathfrak{g}}{t_o n_o k \mathfrak{G}} = \pm\frac{1-\xi^2}{\xi}$$

In any case, we have $\mathfrak{g}/(t_o n_o k \mathfrak{G}) \in \mathbb{Q}_N \cap \mathbb{Q}_8$. If N is odd, then $\mathbb{Q}_N \cap \mathbb{Q}_8 = \mathbb{Q}$ by [74], Prop. 2.4, p. 11. If $N \equiv 2 \pmod 4$, we have $N = 2N'$ for an odd number N', so that $\mathbb{Q}_N = \mathbb{Q}_{N'}$ and again $\mathbb{Q}_N \cap \mathbb{Q}_8 = \mathbb{Q}$ by the same argument. In both cases, we get that $\mathfrak{g}/(t_o n_o k \mathfrak{G})$ is a rational number whose square is ± 2, which is a contradiction. Therefore, $N \equiv 0 \pmod 4$. $\square$

Although the preceding argument is sufficient to prove the assertion, it is worth noting that in the second case, where $\mathfrak{g}^2 = t_o^4 \mathfrak{g}'^2$, we actually get the stronger statement that $N \equiv 0 \pmod 8$. To see this, note that, because we now know that N is divisible by 4, we have $\xi^2 \in \mathbb{Q}_N$, and we have seen in the proof that

$$\frac{1+\xi^2}{\xi} \in \mathbb{Q}_N \qquad \text{or} \qquad \frac{1-\xi^2}{\xi} \in \mathbb{Q}_N$$

Both equations clearly imply that $\xi \in \mathbb{Q}_N$, so that N must be divisible by 8.

This fact is worth pointing out because it appears that, under the assumptions made in the corollary, we always have that N divides n^2. We are therefore lead to conjecture the following stronger form of the corollary:

Conjecture Consider a projective congruence datum that is also Galois. If N denotes its exponent and n its global dimension, then we have

1. $N \equiv 4 \pmod 8$

2. $\mathfrak{g}^2 = -t_o^4 \mathfrak{g}'^2$

if $n \equiv 2 \pmod 4$.

The preceding argument at least shows that the first statement implies the second. Note that in the normalized case the second statement asserts that $\mathfrak{g}'/\mathfrak{g}$ is a primitive fourth root of unity. We will see in Paragraph 5.6 an example where all the assumptions, and therefore all the conclusions, made in this paragraph are satisfied: We there have that $n = 2$, $N = 4$, $t_o = 1$, and $\mathfrak{g}^2 = -\mathfrak{g}'^2$.

4 Hopf Algebras

4.1 Modular data axiomatize certain properties of modular categories, as we explain now. A modular category in the sense of V. G. Turaev (cf. [73], Sec. II.1.4, p. 74) comes with a finite family $(V_i)_{i \in I}$ of objects such that for one index $o \in I$ the corresponding object V_o is the unit object. It follows from the axioms of a modular category that $K := \mathrm{End}(V_o)$ is always a commutative ring (cf. [73], Sec. II.1.1, p. 72); we assume here that it is an algebraically closed field of characteristic zero. The duality in the category leads to an involution on the index set with the property that $o^* = o$ (cf. [73], p. 75). If the quasisymmetry of the category is denoted by c, then we define the Verlinde matrix $\mathbf{S}$ via

$$s_{ij} = \mathrm{tr}_q(c_{V_{j^*},V_i} \circ c_{V_i,V_{j^*}})$$

where tr_q denotes the categorical trace, or quantum trace, as it is sometimes called (cf. [73], Sec. I.1.5, p. 21; [38], Def. XIV.4.1, p. 354). Note that here we have deviated slightly from the convention in [73], p. 74; we include in Paragraph 4.2 below a table that compares the conventions of a couple of references. The Dehn matrix $\mathbf{T}$ arises from the twist of the category, which acts on the simple object V_i via multiplication by a scalar $t_i \in K$; this number is denoted by v_i in [73], p. 76.

This explains how the structure elements of a modular datum arise from a modular category; however, the axioms that we have given in Definition 1.1 will only be satisfied if the category is in addition semisimple. By this, we mean that the category is K-linear, that the objects V_i above are simple, and that every object is isomorphic to a finite direct sum of some of the objects V_i, possibly with repetitions (cf. [73], Sec. II.4.1, p. 99). For these categories, the fact that the numbers t_i are roots of unity is known as Vafa's theorem (cf. [3], Thm. 3.1.19, p. 57). The equation $t_{i^*} = t_i$ holds by [73], Sec. II.3.3, Eq. (3.3.b), p. 90. As noted in [73], Sec. II.1.4, p. 74f, the Verlinde matrix is always symmetric, and s_{io} is always equal to the categorical dimension of the i-th simple object, which is shown there to be nonzero. In view of [73], Exerc. II.1.9.2, p. 78, all of this also holds after our modification.

Our Axiom 1.1.3 about the form of the inverse of $\mathbf{S}$ is in this setting satisfied by [73], Sec. II.3.8, Eq. (3.8.a), p. 97, resp. Sec. II.3.9, p. 98. Similarly, Axiom 1.1.4 is satisfied in this situation by [73], Sec. II.3.8, Eq. (3.8.c), p. 97. Turaev's version is in fact closer to our constant form of Axiom 1.1.4. Although he gives no name to the Gaussian sum, he also introduces an element that corresponds to our reciprocal Gaussian sum $\mathfrak{g}'$ and denotes it by Δ (cf. [73], Sec. II.1.6, p. 76). However, the term 'Gaussian sum' is often used for this element (cf. [50], Def. 1.1, p. 160), as it reduces to the classical Gaussian sum in certain examples that we will consider in Paragraph 4.4. This is also pointed out by Turaev when he derives his variant of Proposition 1.1.5 (cf. [73], Sec. II.2.4, Eq. (2.4.a), p. 83). Finally, Axiom 1.1.5 about the numbers N_{ij}^k is a property

of modular categories known as the Verlinde formula (cf. [73], Thm. II.4.5.2, p. 106; [3], Thm. 3.1.14, p. 54), which shows that this number is the multiplicity of V_k in the decomposition of $V_i \otimes V_j$ into simple objects, and therefore in particular a nonnegative integer.

Modular data coming from modular categories are always normalized: The fact that $t_o = 1$ is shown in [73], Sec. I.1.2, p. 20, and the equation $n_o = 1$ is shown in [73], Lem. I.1.5.1, p. 22. However, they are not always integral. We therefore now proceed to study a class of semisimple modular categories that lead to integral modular data, namely those coming from factorizable Hopf algebras.

4.2 So, we now consider a semisimple Hopf algebra A with coproduct Δ, counit ϵ, and antipode S over an algebraically closed field K of characteristic zero. We denote the dimension of A by n; note that semisimple Hopf algebras are always finite-dimensional (cf. [71], Cor. 2.7, p. 330; [72], Chap. V, Exerc. 4, p. 108). Furthermore, A is also cosemisimple and the antipode is an involution (cf. [42], Thm. 4, p. 195; [43], Thm. 3.3, p. 276).

We also assume that A is quasitriangular. This means that A possesses a so-called R-matrix, i.e., an invertible element $R = \sum_{i=1}^{k} a_i \otimes b_i \in A \otimes A$ that satisfies $\Delta^{\mathrm{cop}}(a) = R\Delta(a)R^{-1}$ as well as

$$(\Delta \otimes \mathrm{id})(R) = \sum_{i,j=1}^{k} a_i \otimes a_j \otimes b_i b_j \qquad (\mathrm{id} \otimes \Delta)(R) = \sum_{i,j=1}^{k} a_i a_j \otimes b_j \otimes b_i$$

(cf. [38], Def. VIII.2.2, p. 173; [47], Def. 10.1.5, p. 180; [73], Sec. XI.2.1, p. 496). From the R-matrix, we derive two further elements, namely

$$R' := \sum_{i=1}^{k} b_i \otimes a_i \qquad u := \sum_{i=1}^{k} S(b_i) a_i$$

The element u is called the Drinfel'd element; it is always invertible. A is called factorizable if the tensor $R'R$ has maximal rank, i.e., if it cannot be written as a sum of less than n decomposable tensors.

The module category of a semisimple factorizable Hopf algebra is modular: For the objects $(V_i)_{i \in I}$, the Wedderburn structure theorem provides a system of representatives for the isomorphism classes of simple modules with the required properties. The object V_o is chosen to be the base field K, turned into an A-module via the counit. As explained in [73], the duality on the category arises from the antipode S (cf. [73], Sec. XI.1.3, p. 494f; see also [38], Sec. XIV.2, Ex. 1, p. 347), and the quasisymmetry of the category arises from the R-matrix (cf. [73], Sec. XI.2.3, p. 498f; see also [38], Prop. XIII.1.4, p. 318).

Because in our situation the antipode is an involution, the inverse Drinfel'd element u^{-1} can be used as a ribbon element. For this ribbon element, the

categorical trace coincides with the usual trace (cf. [73], Lem. XI.3.3, p. 501; see also [38], Prop. XIV.6.4, p. 363), so that the categorical dimensions coincide with the ordinary dimensions. This implies that the entries of the Verlinde matrix $\mathbf{S}$ are given as

$$s_{ij} = (\chi_i \otimes \chi_{j^*})(R'R)$$

where χ_i denotes the character of V_i. The diagonal entry t_i of the Dehn matrix $\mathbf{T}$ is determined by the condition that u^{-1} acts on V_i as $t_i \operatorname{id}_{V_i}$. The decisive axiom of a modular category to check now is the invertibility of the Verlinde matrix; this axiom follows from factorizability by establishing a version of Axiom 1.1.3 (cf. [64], Rem. 3.4, p. 1895; [68], Prop. 5.3, p. 48).

Because the module category of a semisimple factorizable Hopf algebra is modular, the discussion in Paragraph 4.1 implies that the quintuple $(I, o, {}^*, \mathbf{S}, \mathbf{T})$ is a normalized modular datum. Of course, it is also possible to deduce this directly from the definition of a factorizable Hopf algebra (cf. [68], Sec. 5). But the important new feature now is that these modular data are always integral: Because $\chi_o = \epsilon$, it follows from fundamental properties of R-matrices (cf. [47], Prop. 10.1.8, p. 180; [38], Thm. VIII.2.4, p. 175; [73], Lem. XI.2.1.1, p. 497) that

$$s_{io} = (\chi_i \otimes \epsilon)(R'R) = \chi_i(1) = \dim(V_i)$$

so that $n_i = s_{io} = \dim(V_i)$ is the dimension of a vector space, and therefore a positive integer.

The various quantities that we have associated with a modular datum reappear in a slightly different form in the Hopf algebra situation. It follows directly from the Wedderburn structure theorem that the global dimension n of the modular datum is equal to the dimension of the Hopf algebra. The exponent N of the modular datum is obviously equal to the order of the Drinfel'd element u. It is also equal to the exponent as originally defined in terms of Sweedler powers (cf. [34], p. 1261; [35], p. 159; [19], Def. 2.1, p. 132), although this is not completely obvious: It follows by combining [19], Thm. 2.5, p. 133; [35], Thm. 3.4, p. 170, and [68], Lem. 3.1, p. 22.

The Gaussian sum $\mathfrak{g} = \sum_{i \in I} n_i^2 t_i$ also admits another description in the Hopf algebra setting: It again follows from the Wedderburn structure theorem that, for an element $a \in A$, the trace $\chi_R(a)$ of the left multiplication by a is equal to $\chi_R(a) = \sum_{i \in I} n_i \chi_i(a)$. The function χ_R is called the character of the regular representation; it is also a left and right integral on A (cf. [43], Prop. 2.4, p. 273). Because u^{-1} acts on V_i as $t_i \operatorname{id}_{V_i}$, we have $\chi_i(u^{-1}) = n_i t_i$, which implies that $\mathfrak{g} = \chi_R(u^{-1})$; similarly, we see that $\mathfrak{g}' = \chi_R(u)$. As a consequence, the fusion symbol $\mathfrak{f}(q)$ reduces to the Hopf symbol $\left(\frac{q}{A}\right)$ in this case (cf. [68], Def. 12.1, p. 114), and Proposition 1.1.5 becomes $\chi_R(u^{-1})\chi_R(u) = \dim(A)$ (cf. [68], Par. 5.3, p. 49).

To facilitate the comparison between the different conventions used in the various references, we include the following table:

Present notation	[73]	[3]	[68]
s_{ij}	S_{ij^*} (p. 74)	$\tilde{s}_{ij}$ (p. 47)	s_{ij^*} (p. 45)
t_i	v_i (p. 76)	θ_i (p. 44)	$1/u_i$ (p. 45)
n_i	$\dim(i)$ (p. 74)	d_i (p. 44)	n_i (p. 43)
$\mathfrak{g}$	$\Delta_{\bar{\mathcal{V}}}$ (p. 21)	p_+ (p. 49)	$\chi_R(u^{-1})$ (p. 43)
$\mathfrak{g}'$	$\Delta = \Delta_{\mathcal{V}}$ (p. 77)	p_- (p. 49)	$\chi_R(u)$ (p. 43)
D	$\mathcal{D}$ (p. 76)	D (p. 51)	$1/\kappa$ (p. 90)
ℓ		ζ (p. 51)	
N_{ij}^k	h_k^{ij} (p. 105)	N_{ij}^k (p. 44)	

4.3　　We are now in the position to present the main result of this article:

Theorem　　Consider a semisimple factorizable Hopf algebra A over a field K of characteristic zero. Let n be the dimension of A, u its Drinfel'd element, and χ_R the character of its regular representation. Then the following holds:

1. If n is odd, then we have

$$\chi_R(u^{-1}) = \begin{cases} \chi_R(u) & : n \equiv 1 \pmod 4 \\ -\chi_R(u) & : n \equiv 3 \pmod 4 \end{cases}$$

   Moreover, the Hopf symbol coincides with the Jacobi symbol; i.e., we have

$$\left(\frac{q}{A}\right) = \left(\frac{q}{n}\right)$$

   for all $q \in \mathbb{Z}$.

2. If n is even, then we have $\chi_R(u^{-1})^4 = \chi_R(u)^4$.

Proof.　　Because these identities will still hold when we enlarge the base field, we can assume that K is algebraically closed, so that the discussion in Paragraph 4.2 applies. We know that the exponent N of a semisimple Hopf algebra is odd if and only if its dimension n is odd (cf. [19], Thm. 4.3, p. 136; [36], Cor. 4, p. 93), and therefore the equation $\chi_R(u^{-1}) = (-1)^{(n-1)/2}\chi_R(u)$ in the first assertion follows directly from Theorem 2.6. Even stronger, Cauchy's theorem for Hopf algebras implies that N and n have the same prime divisors (cf. [37], Thm. 3.4, p. 26), so that an integer q is relatively prime to N if and only if it is relatively prime to n. Therefore, the equation $\left(\frac{q}{A}\right) = \left(\frac{q}{n}\right)$ also follows from Theorem 2.6.

The second assertion follows similarly from Theorem 3.4: By the projective congruence subgroup theorem, modular data coming from semisimple factorizable Hopf algebras are projective congruence data, and they are also Galois (cf. [68], Thm. 9.4, p. 94, Lem. 12.2, p. 115). □

We have already discussed in Paragraphs 2.5, 2.6, and 3.4 that, in the case $K = \mathbb{C}$, this theorem means that the additive central charge c is always an integer, and an even integer if n is odd. The result is also consistent with a known fact about the Drinfel'd double: If $A = D(H)$ is the Drinfel'd double of an odd-dimensional semisimple Hopf algebra H, then $n = \dim(H)^2$ is a square, and therefore congruent to 1 modulo 4. But in this case, it is known that $\chi_R(u) = \chi_R(u^{-1}) = \dim(H)$ (cf. [50], Prop. 5.18, p. 199; [68], Par. 6.1, p. 53).

However, we do not believe that the preceding theorem is the best possible result. Rather, we expect the following:

Conjecture Consider a semisimple factorizable Hopf algebra A over a field K of characteristic zero. Let n be the dimension of A, u its Drinfel'd element, and χ_R the character of its regular representation. If n is even, then n is divisible by 4. Moreover, we have $\chi_R(u^{-1})^2 = \chi_R(u)^2$.

Using the arguments of the proof of the preceding theorem together with Corollary 3.5, the first part of this conjecture would follow from a conjecture of Y. Kashina, who conjectured that the exponent N of A always divides the dimension n (cf. [34], p. 1261). The best known result on this conjecture is a theorem by P. Etingof and S. Gelaki, which asserts that N divides n^3 (cf. [19], Thm. 4.3, p. 136). However, both Kashina's conjecture and our conjecture do not hold for quasi-Hopf algebras, as we will see in Paragraph 5.6 in an explicit example.

4.4 We have promised in Paragraph 2.6 to explain why the Gaussian sum of a modular datum carries this name. Part of this explanation has been given there already, when we saw that the Gaussian sum of a modular datum is often equal to the classical Gaussian sum. Here, we now give an example of a modular datum whose Gaussian sum is exactly the classical one; the name in the general case comes from this example.

Originally, this example was given by D. E. Radford (cf. [60], Sec. 3, p. 10; [61], Sec. 2.1, p. 219); we have already contemplated it in this context in [68], Par. 5.5, p. 50, and we will use some of the computations carried out there. Consider a cyclic group G of order n. Denote the group ring by $A = K[G]$, and fix a generator g of G. As A is cocommutative, A is certainly quasitriangular with respect to the R-matrix $1 \otimes 1$. However, with respect to this R-matrix, it is not factorizable. Radford has determined all possible R-matrices for A, and shown that A can only be factorizable if n is odd, what we will assume for the rest of this paragraph, and that in this case the R-matrix necessarily has the form

$$R = \frac{1}{n} \sum_{i,j=0}^{n-1} \zeta^{-ij} g^i \otimes g^j$$

where ζ is a primitive n-th root of unity (cf. [61], Sec. 2.3, p. 227).

The claim that the Gaussian sum $\mathfrak{g}$ of the modular datum that arises from this factorizable Hopf algebra is equal to the classical Gaussian sum $\mathfrak{G}$ as introduced in Definition 2.6 now follows directly from the formulas for the Drinfel'd element in this example (cf. [61], Sec. 2.1, p. 219; Sec. 2.3, p. 227; [68], Par. 5.5, p. 51): We get that

$$\chi_R(u^{-1}) = \mathfrak{G} = \sum_{i=0}^{n-1} \zeta^{i^2} \qquad\qquad \chi_R(u) = \mathfrak{G}' = \sum_{i=0}^{n-1} \zeta^{-i^2}$$

Also, by using [59], Chap. 11, Eq. (11.14), p. 89, we observed in [68], Prop. 5.5, p. 51 that the Hopf symbol coincides with the Jacobi symbol in this example; a fact that motivated the definition of the Hopf symbol in the general case (cf. [68], Def. 14.1, p. 114). As a consequence, we observed there that by the first supplement to Jacobi's reciprocity law we have in this example that

$$\chi_R(u^{-1}) = \begin{cases} \chi_R(u) & \text{if} \quad n \equiv 1 \pmod 4 \\ -\chi_R(u) & \text{if} \quad n \equiv 3 \pmod 4 \end{cases}$$

Theorem 4.3 should therefore be seen as a generalization of these two properties from this specific example to arbitrary odd-dimensional semisimple factorizable Hopf algebras.

5 Quasi-Hopf Algebras

5.1   Theorem 4.3 can be partially generalized to quasi-Hopf algebras. Although we will present the corresponding result, our main focus is in a different direction: Quasi-Hopf algebras provide an example of a normalized integral modular datum for which $\mathfrak{g}^4 = \mathfrak{g}'^4$, but $\mathfrak{g}^2 \neq \mathfrak{g}'^2$. In other words, this analogue of Theorem 4.3, and also Theorem 3.4, cannot be improved, and the analogue of Conjecture 4.3 for quasi-Hopf algebras is false.

Quasi-Hopf algebras were introduced by V. G. Drinfel'd in [16]. We will use the setup from [38], Chap. XV; however, we will assume that the unit constraints are trivial, i.e., that the elements denoted by r and l in [38], Prop. XV.1.2, p. 369 are equal to 1. An algebra A over the field K is therefore called a quasi-Hopf algebra if it is equipped with algebra homomorphisms $\Delta : A \to A^{\otimes 2} = A \otimes A$, $\epsilon : A \to K$, and $S : A \to A^{\mathrm{op}}$, called the coproduct, the counit, and the antipode, and elements $\Phi \in A^{\otimes 3}$, $\alpha \in A$, and $\beta \in A$ such that the axioms (1.1)–(1.4) in [38], Prop. XV.1.2, p. 369 as well as the axioms (5.1) and (5.2) in [38], Def. XV.5.1, p. 379 are satisfied; in particular, Φ is assumed to be invertible. Note that these axioms imply that A is an ordinary Hopf algebra if Φ, α, and β are trivial in the sense that they are the unit elements in $A^{\otimes 3}$ resp. A. The element Φ is called the associator of A. We furthermore require that the antipode of A is bijective. We note that the antipode is compatible with the comultiplication in the sense that

$$\Delta(S(a)) = F^{-1}(S \otimes S)(\Delta^{\mathrm{cop}}(a))F$$

(cf. [16], Prop. 1.2, p. 1426), where $F \in A^{\otimes 2}$ is an invertible element that is explicitly given in terms of the defining structure elements (cf. [16], Eq. (1.36), p. 1429). Following the notational conventions of Paragraph 4.2, we denote by F' the image of F under the interchange of the two tensor factors.

We also assume that A is quasitriangular. As in Paragraph 4.2, this means that A is equipped with an R-matrix $R = \sum_i a_i \otimes b_i \in A^{\otimes 2}$; however, the axioms given there must be modified as indicated in [38], Prop. XV.2.2, p. 371. Note that the two sets of axioms coincide in the Hopf algebra case, where the associator is trivial. As explained in [38], p. 380, these structure elements can be used to turn the category of finite-dimensional left A-modules into an autonomous quasisymmetric category, where we, slightly deviating from [38], not require that autonomous categories be strict.

The Drinfel'd element u that we considered in Paragraph 4.2 can also be generalized to the quasi-Hopf algebra setting: It is then defined as

$$u = \sum_{i,j} S(b_i y_j \beta S(z_j)) \alpha a_i x_j$$

where we have used the notation $\Phi^{-1} = \sum_j x_j \otimes y_j \otimes z_j$. It has the following properties:

Proposition u is invertible. Moreover, we have

1. $\epsilon(u) = 1$

2. $S^2(a) = uau^{-1}$

3. $\Delta(u) = F^{-1}((S \otimes S)(F'))(u \otimes u)(R'R)^{-1}$

Proof.   The invertibility of u as well as the first and the second property are proved in [1], Sec. 3, p. 87f. The third property is also proved there (cf. Eq. (4.21), p. 95) under the assumption that α is invertible. However, it was shown in [9], Eq. (3.6), p. 668 that this condition is unnecessary. Note that R' was defined in Paragraph 4.2; the element F comes from the compatibility condition between coproduct and antipode mentioned above. $\square$

The quasi-Hopf algebra A that we are considering will also be assumed to be a ribbon quasi-Hopf algebra, i.e., to be endowed with a ribbon element. This means the following:

Definition   A nonzero central element $v \in A$ is called a ribbon element if it satisfies
$$\Delta(v) = (R'R)(v \otimes v) \quad \text{and} \quad S(v) = v$$

We note that most authors use the inverse of this element as a ribbon element; for example, this is the convention in [38], Def. XIV.6.1, p. 361. Our convention is the one used in [73], Sec. XI.3.1, p. 500. Ribbon elements are not unique: From a given ribbon element, we can construct another one by multiplying it with a central grouplike element that is invariant under the antipode. On the other hand, this is obviously the only possible modification.

The basic properties of ribbon elements are given in the following corollary to the preceding proposition, which is proved in [69]:

Corollary   A ribbon element v is invertible and satisfies $\epsilon(v) = 1$ as well as
$$v^{-2} = uS(u)$$

This corollary in particular asserts that two of the axioms for ribbon quasi-Hopf algebras listed in [9], Thm. 3.1, p. 667, namely Axiom (3.1) and Axiom (3.3), are actually consequences of the other axioms, namely Axiom (3.2) and Axiom (3.5). The axioms listed in [9] were an improved version of the original ones given in [1], Par. 4.1, p. 89.

For an A-module V, we define its twist θ_V as
$$\theta_V : V \to V, \ x \mapsto \theta_V(x) := vx$$

Because v is central, θ_V is A-linear, and therefore the collection of all twists defines a natural transformation from the identity functor to itself. From this and the other axioms for a ribbon element, it follows that these twists turn the category of finite-dimensional A-modules into a ribbon category (cf. [38], Def. XIV.3.2, p. 349; [73], Sec. I.1.4, p. 21). Accordingly, as already pointed out in Paragraph 4.1, every A-linear map $f : V \to V$ has a categorical trace $\mathrm{tr}_q(f)$. The categorical trace of f can be related to the ordinary trace by introducing the map

$$f_q : V \to V, \ x \mapsto f(S(\alpha)uv\beta x)$$

As explained in [1], Par. 4.4, p. 95, the ordinary trace of this map is equal to the categorical trace of f; in other words:

Lemma $\mathrm{tr}_q(f) = \mathrm{tr}(f_q)$

We also note that the version of this lemma for ordinary Hopf algebras, which we have already used in Paragraph 4.3, can be found in [38], Prop. XIV.6.4, p. 363 and [73], Lem. XI.3.3, p. 501.

5.2 On our ribbon quasi-Hopf algebra A, we now impose a number of additional assumptions: First, we assume that the base field K is algebraically closed of characteristic zero. Second, we assume that A is of finite dimension n and semisimple as an algebra. As for ordinary Hopf algebras in Paragraph 4.2, the Wedderburn structure theorem then provides us with a family of simple modules $(V_i)_{i \in I}$, one of which, denoted V_o, is equal to the base field K, turned into an A-module via the counit. The category of finite-dimensional A-modules is therefore a semisimple ribbon category; it will be modular if the Verlinde matrix $\mathbf{S}$ from Paragraph 4.1 is invertible, as we from now on assume. Finally, we assume that $v^{-1} = S(\alpha)u\beta$. We will comment below on the meaning of this assumption; for the moment, we only note that it implies that the categorical trace agrees with the ordinary trace, because we then have $f = f_q$ in Lemma 5.1. As in Paragraph 4.2, the entries of the Verlinde matrix $\mathbf{S}$ are therefore given as

$$s_{ij} = (\chi_i \otimes \chi_{j^*})(R'R)$$

where χ_i denotes the character of V_i and $i^* \in I$ is the unique index satisfying $V_{i^*} \cong V_i^*$.

The remaining parts of the discussion in Paragraph 4.2 also carry over: The diagonal entry t_i of the Dehn matrix $\mathbf{T}$ is determined by the condition that v acts on V_i as $t_i \, \mathrm{id}_{V_i}$, so that we arrive again at a normalized modular datum $(I, o, {}^*, \mathbf{S}, \mathbf{T})$. Using the same computation as in Paragraph 4.2, we get that $n_i = s_{io} = \dim(V_i)$, the dimension of a vector space, so that this modular datum is again integral. As before, the Wedderburn structure theorem implies that the global dimension n of the modular datum is equal to the dimension of A, and the exponent N of the modular datum is again equal to the order of the

ribbon element v. Another consequence of the Wedderburn structure theorem is that the character of the regular representation is given by the formula $\chi_R(a) = \sum_{i \in I} n_i \chi_i(a)$, so that the Gaussian sum $\mathfrak{g} = \sum_{i \in I} n_i^2 t_i$ becomes $\mathfrak{g} = \chi_R(v)$, and the reciprocal Gaussian sum becomes $\mathfrak{g}' = \chi_R(v^{-1})$, exactly as in Paragraph 4.2, where we had $v = u^{-1}$. We can therefore express the fusion symbol $\mathfrak{f}(q)$ again in terms of powers of the ribbon element, and also reformulate Proposition 1.1.5 as the statement $\chi_R(v)\chi_R(v^{-1}) = \dim(A)$.

Let us now try to put our assumption $v^{-1} = S(\alpha)u\beta$ into context. We first note that this assumption has the following consequence:

Proposition A is involutory.

Proof. By definition (cf. [8], Def. 3.1, p. 263), we have to show that

$$S^2(a) = (S(\beta)\alpha) \, a \, (\beta S(\alpha))$$

By assumption, we have $v^{-1} = S(\alpha)u\beta = S(\alpha)S^2(\beta)u$ and therefore

$$S(\beta)\alpha = S^{-1}(v^{-1}u^{-1}) = S^{-1}(u^{-1})v^{-1} = S(u^{-1})v^{-1}$$

Since A is finite-dimensional, this shows that α and β are invertible. From Proposition 5.1, we also have $S^2(a) = S(u)^{-1}aS(u)$. Because v is central, this implies

$$(S(\beta)\alpha) \, a = S(u^{-1})v^{-1} \, a = S^2(a) \, S(u^{-1})v^{-1} = S^2(a) \, (S(\beta)\alpha)$$

Therefore, our assertion will follow if we can show that $S(\beta)\alpha = (\beta S(\alpha))^{-1}$. Solving the assumption $v^{-1} = S(\alpha)u\beta$ for u, we get

$$u = S(\alpha)^{-1}v^{-1}\beta^{-1} = S(\alpha)^{-1}\beta^{-1}v^{-1}$$

But by Corollary 5.1, we have $v^{-2} = uS(u)$, so that

$$S(\alpha)^{-1}\beta^{-1} = uv = S(u^{-1})v^{-1} = S(\beta)\alpha$$

by the first computation above. $\square$

The nature of our assumption becomes clearer when restated in categorical terms: In every left rigid quasisymmetric monoidal category, i.e., a quasisymmetric monoidal category with left duality, there is a canonical natural transformation between the identity functor and the double dual functor $V \mapsto V^{**}$. In the case of the category of finite-dimensional modules over a quasitriangular quasi-Hopf algebra A, this is the natural transformation $V \to V^{**}$, $x \mapsto \Theta(ux)$, where Θ is the isomorphism between V and its double dual from linear algebra, defined as $\Theta(x)(\varphi) = \varphi(x)$ for $x \in V$ and $\varphi \in V^*$. However, this is not a monoidal transformation, but rather a ribbon transformation (cf. [67], Def. 3.2, p. 439), which is reflected by the identities in Proposition 5.1. Monoidal transformations between the identity functor and the double dual functor can also be obtained from elements $w \in A$; however, in comparison to Proposition 5.1, such an element w should satisfy

1. $\epsilon(w) = 1$

2. $S^2(a) = waw^{-1}$

3. $\Delta(w) = F^{-1}((S \otimes S)(F'))(w \otimes w)$

(cf. [8], Prop. 4.2, p. 273; [44], Thm. 7.1, p. 182; [65], Rem. 3.3, p. 133). We then get a monoidal transformations between the identity functor and the double dual functor by assigning to every object V the morphism $V \to V^{**}$, $x \mapsto \Theta(wx)$. If w is invertible, then this will be a natural equivalence, i.e., a pivotal structure. It is now obvious from Proposition 5.1 and the definition of a ribbon element that the element $w := uv$ satisfies these equations. Taking a second look at the preceding proof, we see that our condition $v^{-1} = S(\alpha)u\beta$ is equivalent to the requirement that $w = S(\beta)\alpha$; in other words, we are using the unique pivotal structure for which categorical traces and ordinary traces coincide (cf. [8], Prop. 4.3, p. 275; [21], Prop. 8.23, Prop. 8.24, p. 622f).

5.3   For a quasi-Hopf algebra A that satisfies the assumptions in Paragraph 5.2, the methods developed in Section 2 now apply in the same way as they applied to an ordinary Hopf algebra in Paragraph 4.3, and we get the following result:

Theorem   If the dimension n of A is odd, we have

$$\chi_R(v^{-1}) = \begin{cases} \chi_R(v) & : n \equiv 1 \pmod 4 \\ -\chi_R(v) & : n \equiv 3 \pmod 4 \end{cases}$$

Moreover, the fusion symbol coincides with the Jacobi symbol; i.e., we have $\mathfrak{f}(q) = \left(\frac{q}{n}\right)$ for all $q \in \mathbb{Z}$.

Proof.   By Cauchy's theorem for quasi-Hopf algebras (cf. [56], Thm. 8.4, p. 63), N and n have the same prime divisors, so N is also odd. Note that it follows from [56], Thm. 7.7, p. 60 that N is the Frobenius-Schur exponent of A. Therefore, the equation $\chi_R(v^{-1}) = (-1)^{(n-1)/2}\chi_R(v)$ follows again directly from Theorem 2.6. Cauchy's theorem also implies that an integer q is relatively prime to N if and only if it is relatively prime to n, which means that $\mathfrak{f}(q) \neq 0$ if and only if $\left(\frac{q}{n}\right) \neq 0$. But as soon as these two numbers are nonzero, they are equal by Theorem 2.6. $\square$

It is difficult to overlook that the preceding theorem does not contain an analogue of the second part of Theorem 4.3, which was concerned with the case where the dimension n is even, despite the fact that the projective congruence subgroup theorem has already been carried over from Hopf algebras (cf. [68], Thm. 9.4, p. 94) to quasi-Hopf algebras (cf. [57], Thm. 8.8, p. 35). The reason for this is that the Galois property (cf. [68], Lem. 12.2, p. 115) has not yet been carried over. However, we expect that this property can also be established for

quasi-Hopf algebras in an analogous way, so that then the methods of Section 3 would apply and we would get that $\chi_R(v^{-1})^4 = \chi_R(v)^4$ for any quasi-Hopf algebra that satisfies the conditions in Paragraph 5.2.

On the other hand, we have explicitly formulated in Conjecture 4.3 our expectation that, in the Hopf algebra case, we even have the stronger result that $\chi_R(v^{-1})^2 = \chi_R(v)^2$. This result, if correct, at least does not carry over to quasi-Hopf algebras, as we will show now by an explicit example.

5.4 In general, if G is a finite group and $\omega : G \times G \times G \to K^\times$ is a normalized 3-cocycle (cf. [38], Sec. XV.5, Eq. (5.3), p. 380), then the dual group ring $K[G]^*$, which is an ordinary Hopf algebra, can also be considered as a quasi-Hopf algebra with respect to the associator

$$\Phi = \sum_{g,h,k \in G} \omega(g,h,k) \, e_g \otimes e_h \otimes e_k$$

and the antipode elements

$$\alpha = 1 \qquad\qquad \beta = \sum_{g \in G} \omega(g^{-1}, g, g^{-1}) \, e_g$$

where e_g is the dual basis element of $g \in G \subset K[G]$ (cf. [29], App. A, p. 585; [55], Sec. 7, p. 1856). In particular, if $G = \mathbb{Z}_n$ is the cyclic group of order n, which we represent in the form $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$, we can construct such a cocycle in the following way: For $i, j \in \{0, 1, 2, \ldots, n-1\}$, we define

$$q_{ij} := \frac{1}{n}(\bar{i} + \bar{j} - \overline{i+j}) = \begin{cases} 0 & : i + j \leq n-1 \\ 1 & : i + j \geq n \end{cases}$$

where, for $i \in \mathbb{Z}$, the element $\bar{i} \in \{0, 1, 2, \ldots, n-1\}$ is the unique number that satisfies $i \equiv \bar{i} \pmod{n}$. Then the function

$$\sigma : \mathbb{Z}_n \times \mathbb{Z}_n \to K^\times, \ (i,j) \mapsto \sigma(i,j) := \zeta^{q_{ij}}$$

where ζ is an n-th root of unity, is a normalized 2-cocycle (cf. [32], Chap. I, § 15, p. 80), and from this it is comparatively easy to see that

$$\omega : \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n \to K^\times, \ (i,j,k) \mapsto \omega(i,j,k) := \sigma(i,j)^k$$

is a normalized 3-cocycle. Further details on this discussion and related material can be found in [48], Eq. (E.14), p. 251; [52], Ex. 5.8, p. 265; and [56], Sec. 9, p. 68f.

5.5 The simplest nontrivial case of the above construction is the case $n = 2$. This special case has already been used as an example several times, as in [20],

Par. 2.3, p. 687 and [55], Ex. 5.4, p. 1854. Note that the convention for α and β in [20] slightly deviates from the one used here. As we want $\Phi \neq 1$, we have to choose $\zeta = -1$; we then have

$$q_{ij} = \begin{cases} 0 & : i = 0 \text{ or } j = 0 \\ 1 & : i = 1 \text{ and } j = 1 \end{cases}$$

so that $q_{ij} = ij$ and consequently

$$\sigma(i,j) = (-1)^{ij} \qquad \omega(i,j,k) = (-1)^{ijk}$$

The possible R-matrices for this quasi-Hopf algebra have been determined in [8], Prop. 3.6, p. 265; they have the form

$$R = e_0 \otimes e_0 + e_0 \otimes e_1 + e_1 \otimes e_0 + \iota e_1 \otimes e_1$$

where $\iota \in K$ is a primitive fourth root of unity. Inserting this into the definition in Paragraph 5.1, we find that the Drinfel'd element then is $u = e_0 + \iota e_1$. We also compute the element F that we introduced in Paragraph 5.1:

Lemma
$$F = e_0 \otimes e_0 + e_0 \otimes e_1 + e_1 \otimes e_0 - e_1 \otimes e_1$$

Proof. We have $\alpha = 1 = e_0 + e_1$ and $\beta = e_0 - e_1$. It therefore follows from [16], Eq. (1.35), p. 1429 that F is in our case equal to the element γ defined in [16], Eq. (1.24), p. 1426. Now we have

$$(1 \otimes \Phi^{-1})(\mathrm{id} \otimes \mathrm{id} \otimes \mathrm{id} \otimes \Delta)(\Phi) =$$

$$(\sum_{p,q,r=0}^{1} (-1)^{pqr} \, 1 \otimes e_p \otimes e_q \otimes e_r)(\sum_{i,j,k,l=0}^{1} (-1)^{ij(k+l)} \, e_i \otimes e_j \otimes e_k \otimes e_l) =$$

$$\sum_{i,j,k,l=0}^{1} (-1)^{jkl}(-1)^{ij(k+l)} \, e_i \otimes e_j \otimes e_k \otimes e_l$$

Inserting this into the definition of γ, we find

$$\gamma = \sum_{i,j,k,l=0}^{1} (-1)^{jkl}(-1)^{ij(k+l)} \, S(e_j)\alpha e_k \otimes S(e_i)\alpha e_l$$

$$= \sum_{i,j=0}^{1} (-1)^{j^2 i}(-1)^{ij(j+i)} \, e_j \otimes e_i = \sum_{i,j=0}^{1} (-1)^{ij} \, e_j \otimes e_i$$

as asserted. $\square$

As a consequence, Proposition 5.1.3 implies that $u^{-1} = e_0 - \iota e_1$ is a ribbon element. However, it is not the only one: As we pointed out directly after

Definition 5.1, we can modify a given ribbon element by multiplying it with a central grouplike element that is invariant under the antipode. Therefore, $v := \beta u^{-1} = e_0 + \iota e_1 = u$ is another ribbon element, and this is the one we want, because we want to satisfy the requirement $v^{-1} = S(\alpha)u\beta$ made in Paragraph 5.2.

Let us consider how we can satisfy the other requirements made in Paragraph 5.2. Using $I = \{0, 1\}$ as index set with $o = 0$ as distinguished element, we have two simple modules $V_0 := K \cong Ke_0$ and $V_1 := Ke_1$. Note that Ke_0 and Ke_1 are ideals. The characters χ_0 and χ_1 of these modules satisfy $\chi_i(e_j) = \delta_{ij}$. Because the antipode is the identity in this example, the involution * is also the identity here. The formula $s_{ij} = (\chi_i \otimes \chi_{j^*})(R'R)$ for the entries of the Verlinde matrix given in Paragraph 5.2 therefore implies that this matrix is

$$\mathbf{S} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

so that the last requirement, the invertibility of $\mathbf{S}$, is also met. The form of the Dehn matrix follows directly from the form of the ribbon element given above; we have

$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & \iota \end{pmatrix}$$

5.6 The modular datum that we have just obtained from the quasi-Hopf algebra $K[\mathbb{Z}_2]^*$ also arises from other constructions, for example from the Kac-Moody algebra $A_1^{(1)}$ at level 1 (cf. [26], Sec. 3, Eq. (3.5), p. 223; [27], Sec. 6.2.1, Eq. (6.2.2), p. 368; [33], Chap. 13, Ex. 13.8, p. 265). Following [63], Sec. 5.3, p. 38, we call this datum the semion datum. It is frequently used in the literature; we mention only [18], Sec. 5, p. 655 and [30], Par. 4.1.3, p. 56.

The semion datum is a normalized integral modular datum, like every modular datum that arises from a quasi-Hopf algebra that satisfies the requirements imposed in Paragraph 5.2. Of course, it is also easy to verify the axioms in Definition 1.1 directly. Obviously, the exponent, which is equal to the normalized exponent here, is $N = N_o = 4$, and the global dimension n is 2, the dimension of the quasi-Hopf algebra. For the Gaussian sum, we find $\mathfrak{g} = 1 + \iota$, and for the reciprocal Gaussian sum $\mathfrak{g}' = 1 - \iota$, so that we have $\mathfrak{g}^2 = 2\iota = -\mathfrak{g}'^2$. This shows that Theorem 3.4 cannot be improved, because the semion datum satisfies the hypotheses of that theorem:

Lemma The semion datum is a projective congruence datum that is also Galois.

Proof. The Galois group of the cyclotomic field $\mathbb{Q}_4 \subset K$ contains only one nonidentity element, namely the automorphism γ discussed in Paragraph 1.5. The Galois condition therefore becomes $t_{\gamma.i} = \gamma^2(t_i)$, where $t_0 = 1$ and $t_1 = \iota$. But by Proposition 1.5, we have $\gamma.i = i^* = i$, so that the condition holds.

As we already mentioned in Paragraph 5.3, the projective congruence subgroup theorem for quasi-Hopf algebras implies that the semion datum is a projective congruence datum. In the present case, however, this is easy to see directly, because to obtain $\mathrm{SL}(2, \mathbb{Z}_4)$ from $\mathrm{SL}(2, \mathbb{Z})$, the only defining relation that we need to add is the relation $\bar{\mathfrak{t}}^4 = 1$ (cf. [23], Sec. 3.6, p. 64; [54], Chap. VIII, p. 145ff), which is clearly satisfied in our example. $\square$

However, the projective representation

$$\mathrm{SL}(2, \mathbb{Z}_4) \to \mathrm{PGL}(2, K),\ \bar{\mathfrak{s}} \mapsto \mathbf{S},\ \bar{\mathfrak{t}} \mapsto \mathbf{T}$$

that we have just described cannot be lifted to an ordinary representation of $\mathrm{SL}(2, \mathbb{Z}_4)$. To see this, assume that there is such a representation, and denote the images of the generators $\bar{\mathfrak{s}}$ and $\bar{\mathfrak{t}}$ by $\mathbf{S}'$ and $\mathbf{T}'$. These matrices then have to satisfy the relations

$$\mathbf{S}'^4 = \mathbf{E} \qquad\qquad \mathbf{T}'^4 = \mathbf{E} \qquad\qquad (\mathbf{T}'\mathbf{S}')^3 = \mathbf{S}'^2$$

Because the representation lifts the projective one, there must be nonzero numbers $D, \ell \in K^\times$ such that

$$\mathbf{S}' = \frac{\mathbf{S}}{D} \qquad \text{and} \qquad \mathbf{T}' = \frac{\mathbf{T}}{\ell}$$

Inserting this into the preceding relations, these become

$$\mathbf{S}^4 = D^4 \mathbf{E} \qquad\qquad \mathbf{T}^4 = \ell^4 \mathbf{E} \qquad\qquad (\mathbf{T}\mathbf{S})^3 = D\ell^3 \mathbf{S}^2$$

But we know already that $\mathbf{T}^4 = \mathbf{E}$, and from Axiom 1.1.3 and the constant form of Axiom 1.1.4 we know that $\mathbf{S}^2 = 2\mathbf{E}$ and $(\mathbf{T}\mathbf{S})^3 = \mathfrak{g}\mathbf{S}^2$. Therefore, our conditions imply that

$$D^4 = 4 \qquad\qquad \ell^4 = 1 \qquad\qquad D\ell^3 = \mathfrak{g} = 1 + \iota$$

Raising the last condition to the fourth power, we get

$$4 = (D\ell^3)^4 = (1 + \iota)^4 = (2\iota)^2 = -4$$

a contradiction.

Stated differently, this computation shows that it is not possible to extend the semion datum by choosing a generalized rank D and a (multiplicative) central charge ℓ in such a way that the extended modular datum is a congruence datum. However, the kernel of the linear representation of the modular group that we have associated with any extension in Paragraph 1.7 is still a congruence subgroup, although not of level $N = 4$:

Proposition It is possible to extend the semion datum in such a way that the kernel of the associated linear representation of the modular group contains $\Gamma(8)$. For every extension, this kernel contains $\Gamma(24)$.

Proof. (1) Using the abbreviation $\bar{\mathfrak{d}} = \bar{\mathfrak{d}}(5,5) = \bar{\mathfrak{s}}\bar{\mathfrak{t}}^5\bar{\mathfrak{s}}^{-1}\bar{\mathfrak{t}}^5\bar{\mathfrak{s}}\bar{\mathfrak{t}}^5$ from Definition 3.2, the matrices $\bar{\mathfrak{s}}, \bar{\mathfrak{t}} \in \mathrm{SL}(2, \mathbb{Z}_8)$ satisfy

$$\bar{\mathfrak{t}}^8 = 1 \qquad\qquad \bar{\mathfrak{s}} = \bar{\mathfrak{d}}\bar{\mathfrak{s}}\bar{\mathfrak{d}} \qquad\qquad \bar{\mathfrak{t}} = \bar{\mathfrak{d}}\bar{\mathfrak{t}}\bar{\mathfrak{d}}^{-1}$$

Together with the relations $\bar{\mathfrak{s}}^4 = 1$ and $(\bar{\mathfrak{t}}\bar{\mathfrak{s}})^3 = \bar{\mathfrak{s}}^2$ from Paragraph 1.7, these are defining relations for $\mathrm{SL}(2, \mathbb{Z}_8)$. This follows by transposing the presentation given in [45], Lem. 3.3, p. 210 and noting that the last relation there is equivalent to Equation (3.17) on the following page there.

Now let D be one of the two solutions to the equation $D^2 = -2$, and set $\ell := (1 - \iota)/D$. Then D is a generalized rank that is not a rank. Furthermore, we have $\ell^2 = -2\iota/D^2 = \iota$ and therefore $\ell^3 = (\iota+1)/D = \mathfrak{g}/D$. This shows that ℓ is a multiplicative central charge, so that we get an extended modular datum. As we have discussed in Paragraph 1.7, the associated homogeneous Verlinde matrix $\mathbf{S}' = \mathbf{S}/D$ and the homogeneous Dehn matrix $\mathbf{T}' = \mathbf{T}/\ell$ give rise to a linear representation of the modular group by mapping $\mathfrak{s}$ to $\mathbf{S}'$ and $\mathfrak{t}$ to $\mathbf{T}'$. The kernel of this representation will contain $\Gamma(8)$ if the additional relations stated above are satisfied. Because $\ell^2 = \iota$, we have $\ell^8 = 1$, so $\mathbf{T}'^8 = \mathbf{E}$, which means that the first relation holds.

Because $\iota^5 = \iota$, we have $\mathbf{T}^5 = \mathbf{T}$, and therefore the image of $\mathfrak{d}(5,5)$ under the associated linear representation of the modular group is

$$\frac{1}{D\ell^{15}}\mathbf{S}\mathbf{T}\mathbf{S}^{-1}\mathbf{T}\mathbf{S}\mathbf{T} = \frac{1}{2D\ell^{15}}(\mathbf{S}\mathbf{T})^3 = \frac{\mathfrak{g}}{2D\ell^{15}}\mathbf{S}^2 = \frac{\mathfrak{g}}{D\ell^{15}}\mathbf{E} = \frac{\mathfrak{g}\ell}{D}\mathbf{E} = \ell^4\mathbf{E} = -\mathbf{E}$$

and from this it is obvious that the two remaining relations are also satisfied.

(2) To prove that, for any extension, $\Gamma(24)$ is in the kernel of the associated representation of the modular group, recall that we have $\mathbb{Z}_{24} \cong \mathbb{Z}_8 \times \mathbb{Z}_3$ by the Chinese remainder theorem, and therefore $\mathrm{SL}(2, \mathbb{Z}_{24}) \cong \mathrm{SL}(2, \mathbb{Z}_8) \times \mathrm{SL}(2, \mathbb{Z}_3)$. The group $\mathrm{SL}(2, \mathbb{Z}_8) \times \mathrm{SL}(2, \mathbb{Z}_3)$ is easy to present: It is generated by the four elements $(\bar{\mathfrak{t}}, 1)$, $(\bar{\mathfrak{s}}, 1)$, $(1, \bar{\mathfrak{t}})$, and $(1, \bar{\mathfrak{s}})$. The generators $(\bar{\mathfrak{t}}, 1)$ and $(\bar{\mathfrak{s}}, 1)$ have to satisfy the preceding relations for $\mathrm{SL}(2, \mathbb{Z}_8)$. The generators $(1, \bar{\mathfrak{t}})$ and $(1, \bar{\mathfrak{s}})$ have to satisfy the defining relations for $\mathrm{SL}(2, \mathbb{Z}_3)$, which are those for the modular group stated in Paragraph 1.7 and the relation $(1, \bar{\mathfrak{t}})^3 = (1, 1)$ (cf. [23], Sec. 3.6, p. 64; [54], Chap. VIII, p. 145ff). Finally, each of the first two generators has to commute with each of the latter two.

This presentation translates into a presentation of $\mathrm{SL}(2, \mathbb{Z}_{24})$ if we can find the corresponding generators. For this, note that the isomorphism coming from the Chinese remainder theorem maps $\bar{9} \in \mathbb{Z}_{24}$ to $(\bar{1}, \bar{0}) \in \mathbb{Z}_8 \times \mathbb{Z}_3$, and similarly $\bar{16}$ to $(\bar{0}, \bar{1})$. As a consequence, $\bar{\mathfrak{t}}^9 \in \mathrm{SL}(2, \mathbb{Z}_{24})$ is mapped to the first generator $(\bar{\mathfrak{t}}, 1) \in \mathrm{SL}(2, \mathbb{Z}_8) \times \mathrm{SL}(2, \mathbb{Z}_3)$, and similarly $\bar{\mathfrak{t}}^{16}$ is mapped to $(1, \bar{\mathfrak{t}})$.

To find the preimages of the two remaining generators, note that it follows from Definition 3.2 that $\mathfrak{d}(0,0) = \mathfrak{s}$ and $\mathfrak{d}(1,1) = 1$. Consequently, the element $\bar{\mathfrak{d}}(16, 16) \in \mathrm{SL}(2, \mathbb{Z}_{24})$ is mapped to $(\bar{\mathfrak{s}}, 1) \in \mathrm{SL}(2, \mathbb{Z}_8) \times \mathrm{SL}(2, \mathbb{Z}_3)$, and similarly $\bar{\mathfrak{d}}(9, 9)$ is mapped to $(1, \bar{\mathfrak{s}})$.

(3) Now let D be an arbitrary generalized rank, and ℓ be an arbitrary multiplicative central charge. According to Definition 1.7, this means that $D^4 = n^2 = 4$ and $\ell^3 = \mathfrak{g}/D$, which implies that

$$\ell^{12} = \frac{\mathfrak{g}^4}{D^4} = \frac{1}{4}(1+\iota)^4 = -1$$

As explained in Paragraph 1.7, the associated linear representation of the modular group maps $\mathfrak{s}$ to the homogeneous Verlinde matrix $\mathbf{S}' = \mathbf{S}/D$ and $\mathfrak{t}$ to the homogeneous Dehn matrix $\mathbf{T}' = \mathbf{T}/\ell$. If this representation would factor over $\mathrm{SL}(2, \mathbb{Z}_{24})$, it would therefore map the generator $\bar{\mathfrak{t}}^9$ to $\mathbf{T}'^9 = \mathbf{T}/\ell^9$ and the generator $\bar{\mathfrak{t}}^{16}$ to $\mathbf{T}'^{16} = \mathbf{E}/\ell^{16}$. Using this, we see that it would map the generator $\bar{\mathfrak{d}}(9, 9)$ to $\mathbf{E}$ and the generator $\bar{\mathfrak{d}}(16, 16)$ to $\mathbf{S}' = \mathbf{S}/D$.

This factorization will occur if these potential images satisfy the relations that we have described above. Since the generators $\bar{\mathfrak{t}}^{16}$ and $\bar{\mathfrak{d}}(9, 9)$, which correspond to $(1, \bar{\mathfrak{t}})$ and $(1, \bar{\mathfrak{s}})$, are mapped to multiples of the unit matrix, the commutation property described above is satisfied. The only remaining conditions that these two generators have to satisfy are the defining relations of $\mathrm{SL}(2, \mathbb{Z}_3)$ already outlined above, which here reduce to the condition $(\ell^{16})^3 = 1$, an obvious consequence of $\ell^{12} = -1$.

(4) It remains to check that the images $\mathbf{S}/D = \mathbf{S}'$ and $\mathbf{T}/\ell^9 = \mathbf{T}'/\ell^8$ of the generators that correspond to $(\bar{\mathfrak{s}}, 1)$ and $(\bar{\mathfrak{t}}, 1)$ satisfy the defining relations of $\mathrm{SL}(2, \mathbb{Z}_8)$ described in the first step. Because the relations in $\mathrm{SL}(2, \mathbb{Z})$ hold, we know that $\mathbf{S}'^4 = \mathbf{E}$, and $(\mathbf{T}'\mathbf{S}')^3 = \mathbf{S}'^2$, and these relations still hold if we rescale $\mathbf{T}'$ by $1/\ell^8$ and leave $\mathbf{S}'$ untouched. But as we saw in the first step, there are three additional conditions. The first one is that the order of $\mathbf{T}/\ell^9$ divides 8, which holds because $\mathbf{T}^4 = 1$ and $(\ell^9)^8 = (\ell^{12})^6 = (-1)^6 = 1$. For the remaining two conditions, we need to find, as in the first step, the potential image of $(\bar{\mathfrak{d}}(5, 5), 1)$. This is found by a very similar computation, namely

$$\frac{1}{D\ell^{135}}\mathbf{STS}^{-1}\mathbf{TST} = \frac{1}{2D\ell^{135}}(\mathbf{ST})^3 = \frac{\mathfrak{g}}{2D\ell^{135}}\mathbf{S}^2 = \frac{\mathfrak{g}}{D\ell^{135}}\mathbf{E} = -\mathbf{E}$$

where we have used that $((\ell^9)^5)^3 = \ell^{135} = (\ell^{12})^{11}\ell^3 = (-1)^{11}\ell^3 = -\ell^3 = -\mathfrak{g}/D$. As in the first step, the two remaining conditions are immediate consequences of this fact. $\square$

It is instructive to compare our treatment of the semion datum with the one in [17] and [63]. For this, we again consider the base field $K = \mathbb{C}$ and write, as in Paragraph 1.7, $\ell = e^{2\pi i c/24}$, where c is the additive central charge. Working with the homogeneous versions, Eholzer first considers in [17], Sec. 5.1, p. 638 the matrices

$$\mathbf{S}' = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \qquad \mathbf{T}' = \begin{pmatrix} e^{2\pi i/8} & 0 \\ 0 & e^{2\pi i(3/8)} \end{pmatrix} = \frac{1}{e^{-2\pi i/8}}\begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{pmatrix}$$

Comparing with our language, we see that Eholzer uses $D = -\sqrt{2}$, which is a rank. Furthermore, we see that we have $\iota = e^{\pi i/2} = i$, and $\ell = e^{-2\pi i/8} = e^{2\pi i(21/24)}$, so that the additive central charge is $c = 21$. Although these choices for ℓ and D differ from the ones that we made in the first step of the preceding proof, these choices also entail that $D\ell^3 = 1 + \iota$, and $\ell^4 = -1$, and a second look at the preceding argument shows that this implies that $\Gamma(8)$ lies in the kernel, which is in fact the starting point for Eholzer's construction of the example. The second version of the homogeneous Dehn matrix that Eholzer considers is the complex conjugate of the first, for which we therefore have $c = 3$.

On the other hand, Rowell et al. consider in [63], Sec. 5.3, p. 38 the matrices

$$
\mathbf{S} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
\qquad
\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}
$$

Note that our matrix $\mathbf{S}$ corresponds to their matrix $\tilde{S}$ and our matrix $\mathbf{S}'$ corresponds to their matrix S. They then use $D = \sqrt{2}$, the other rank, and therefore get from their analogue of Definition 1.7 (cf. [63], Prop. 2.6, p. 9) directly $c = 1$ for the central charge. In our terminology, this leads to the choice $\ell = e^{2\pi i/24}$, so that we do not have $\ell^8 = 1$. Accordingly, the kernel of the associated linear representation of the modular group does not contain $\Gamma(8)$, but only $\Gamma(24)$. This distinction is, however, not relevant for the authors, because they only look at the projective representation (cf. [63], p. 44 and p. 47).

Bibliography

[1] D. Altschüler/A. Coste: Quasi-quantum groups, knots, three-manifolds, and topological field theory, Commun. Math. Phys. 150 (1992), 83-107

[2] T. M. Apostol: Modular forms and Dirichlet series in number theory, 2nd ed., Grad. Texts Math., Vol. 41, Springer, Berlin, 1990

[3] B. Bakalov/A. Kirillov Jr.: Lectures on tensor categories and modular functors, Univ. Lect. Ser., Vol. 21, Am. Math. Soc., Providence, 2001

[4] P. Bantay: The kernel of the modular representation and the Galois action in RCFT, Commun. Math. Phys. 233 (2003), 423-438

[5] A. Beauville: Conformal blocks, fusion rules and the Verlinde formula. In: M. Teicher (ed.): Proceedings of the Hirzebruch 65 conference on algebraic geometry, Isr. Math. Conf. Proc., Vol. 9, Bar-Ilan Univ., Ramat-Gan, 1996, 75-96

[6] B. C. Berndt/R. J. Evans/K. S. Williams: Gauss and Jacobi sums, Can. Math. Soc. Ser. Monogr. Adv. Texts, Vol. 21, Wiley, New York, 1998

[7] F. R. Beyl: The Schur multiplicator of $SL(2, \mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property, Math. Z. 191 (1986), 23-42

[8] D. Bulacu/S. Caenepeel/B. Torrecillas: Involutory quasi-Hopf algebras, Algebr. Represent. Theory 12 (2009), 257-285

[9] D. Bulacu/E. Nauwelaerts: Quasitriangular and ribbon quasi-Hopf algebras, Commun. Algebra 31 (2003), 657-672

[10] V. Chari/A. Pressley: A guide to quantum groups, Camb. Univ. Press, Cambridge, 1994

[11] A. Coste/T. Gannon: Congruence subgroups and rational conformal field theory, Preprint, math.QA/9909080, 1999

[12] A. Coste/T. Gannon/P. Ruelle: Finite group modular data, Nuclear Phys. B 581 (2000), 679-717

[13] H. S. M. Coxeter/W. O. J. Moser: Generators and relations for discrete groups, 4th ed., Ergeb. Math. Grenzgeb., Vol. 14, Springer, Berlin, 1984

[14] M. Cuntz: Integral modular data and congruences, J. Algebr. Comb. 29 (2009), 357-387

[15] J. de Boer/J. Goeree: Markov traces and II_1 factors in conformal field theory, Commun. Math. Phys. 139 (1991), 267-304

[16] V. G. Drinfel'd: Quasi-Hopf algebras, Leningrad Math. J. 1 (1990), 1419-1457

[17] W. Eholzer: On the classification of modular fusion algebras, Commun. Math. Phys. 172 (1995), 623-659

[18] P. Etingof: On Vafa's theorem for tensor categories, Math. Res. Lett. 9 (2002), 651-657

[19] P. Etingof/S. Gelaki: On the exponent of finite-dimensional Hopf algebras, Math. Res. Lett. 6 (1999), 131-140

[20] P. Etingof/S. Gelaki: Finite dimensional quasi-Hopf algebras with radical of codimension 2, Math. Res. Lett. 11 (2004), 685-696

[21] P. Etingof/D. Nikshych/V. Ostrik: On fusion categories, Ann. Math., II. Ser., 162 (2005), 581-642

[22] B. Farb/R. K. Dennis: Noncommutative algebra, Grad. Texts Math., Vol. 144, Springer, Berlin, 1993

[23] B. Fine: Algebraic theory of the Bianchi groups, Pure Appl. Math., Vol. 129, Dekker, New York, 1989

[24] B. Fine/G. Rosenberger: Number theory, Birkhäuser, Basel, 2007

[25] H. Frasch: Die Erzeugenden der Hauptkongruenzuntergruppen für Primzahlstufen, Math. Ann. 108 (1933), 229-252

[26] T. Gannon: Modular data: the algebraic combinatorics of conformal field theory, J. Algebr. Comb. 22 (2005), 211-250

[27] T. Gannon: Moonshine beyond the monster, Camb. Monogr. Math. Phys., Camb. Univ. Press, Cambridge, 2006

[28] C. F. Gauß: Summatio quarumdam serierum singularium, Comm. Soc. reg. sci. Gottingensis rec. 1 (1811)

[29] F. Haußer/F. Nill: Doubles of quasi-quantum groups, Commun. Math. Phys. 199 (1999), 547-589

[30] S. Hu: Lecture notes on Chern-Simons-Witten theory, World Scientific, Singapore, 2001

[31] B. Huppert: Endliche Gruppen I, Grundlehren Math. Wiss., Vol. 134, Springer, Berlin, 1979

[32] N. Jacobson: Lectures in abstract algebra III: Theory of fields and Galois theory, Grad. Texts Math., Vol. 32, Springer, Berlin, 1976

[33] V. G. Kac: Infinite dimensional Lie algebras, 3rd ed., Camb. Univ. Press, Cambridge, 1990

[34] Y. Kashina: On the order of the antipode of Hopf algebras in $_H^H YD$, Commun. Algebra 27 (1999), 1261-1273

[35] Y. Kashina: A generalized power map for Hopf algebras. In: S. Caenepeel/ F. van Oystaeyen (ed.): Hopf algebras and quantum groups, Lect. Notes Pure Appl. Math., Vol. 209, Dekker, New York, 2000, 159-175

[36] Y. Kashina/Y. Sommerhäuser/Y. Zhu: Self-dual modules of semisimple Hopf algebras, J. Algebra 257 (2002), 88-96

[37] Y. Kashina/Y. Sommerhäuser/Y. Zhu: On higher Frobenius-Schur indicators, Mem. Am. Math. Soc., Vol. 181, No. 855, Am. Math. Soc., Providence, 2006

[38] C. Kassel: Quantum groups, Grad. Texts Math., Vol. 155, Springer, Berlin, 1995

[39] C. Kassel/V. G. Turaev: Braid groups, Grad. Texts Math., Vol. 247, Springer, Berlin, 2008

[40] F. Klein/R. Fricke: Vorlesungen über die Theorie der elliptischen Modulfunktionen, 1. Band, Teubner, Stuttgart, 1890

[41] E. Landau: Elementary number theory, 2nd ed., Chelsea, New York, 1966

[42] R. G. Larson/D. E. Radford: Semisimple cosemisimple Hopf algebras, Am. J. Math. 109 (1987), 187-195

[43] R. G. Larson/D. E. Radford: Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, J. Algebra 117 (1988), 267-289

[44] G. Mason/S.-H. Ng: Central invariants and Frobenius-Schur indicators for semisimple quasi-Hopf algebras, Adv. Math. 190 (2005), 161-195

[45] J. Mennicke: On Ihara's modular group, Invent. Math. 4 (1967), 202-228

[46] F. Mertens: Über die Gaussischen Summen, Berl. Ber. (1896), 217-219

[47] S. Montgomery: Hopf algebras and their actions on rings, 2nd revised printing, Reg. Conf. Ser. Math., Vol. 82, Am. Math. Soc., Providence, 1997

[48] G. Moore/N. Seiberg: Classical and quantum conformal field theory, Commun. Math. Phys. 123 (1989), 177-254

[49] M. Müger: From subfactors to categories and topology I: Frobenius algebras in and Morita equivalence of tensor categories, J. Pure Appl. Algebra 180 (2003), 81-157

[50] M. Müger: From subfactors to categories and topology II: The quantum double of tensor categories and subfactors, J. Pure Appl. Algebra 180 (2003), 159-219

[51] T. Nagell: Introduction to number theory, Chelsea, New York, 1964

[52] S. Natale: On the exponent of tensor categories coming from finite groups, Israel J. Math. 162 (2007), 253-273

[53] J. Neukirch: Algebraische Zahlentheorie, Springer, Berlin, 1992

[54] M. Newman: Integral matrices, Pure Appl. Math., Vol. 45, Academic Press, New York, 1972

[55] S.-H. Ng/P. Schauenburg: Central invariants and higher Frobenius-Schur indicators for semisimple quasi-Hopf algebras, Trans. Am. Math. Soc. 360 (2008), 1839-1860

[56] S.-H. Ng/P. Schauenburg: Frobenius-Schur indicators and exponents of spherical categories, Adv. Math. 211 (2007), 34-71

[57] S.-H. Ng/P. Schauenburg: Congruence subgroups and generalized Frobenius-Schur indicators, Preprint, arXiv:0806.2493v1 [math.QA], 2008

[58] W. D. Nichols/M. B. Richmond: The Grothendieck algebra of a Hopf algebra I, Commun. Algebra 26 (1998), 1081-1095

[59] H. Rademacher: Lectures on elementary number theory, Blaisdell, New York, 1964

[60] D. E. Radford: On the antipode of a quasitriangular Hopf algebra, J. Algebra 151 (1992), 1-11

[61] D. E. Radford: On Kauffman's knot invariants arising from finite-dimensional Hopf algebras. In: J. Bergen/S. Montgomery (ed.): Advances in Hopf algebras, Lect. Notes Pure Appl. Math., Vol. 158, Dekker, New York, 1994, 205-266

[62] J. J. Rotman: An introduction to homological algebra, Pure Appl. Math., Vol. 85, Academic Press, New York, 1979

[63] E. Rowell/R. Stong/Z. Wang: On classification of modular tensor categories, Preprint, arXiv:0712.1377v3 [math.QA], 2007

[64] H.-J. Schneider: Some properties of factorizable Hopf algebras, Proc. Am. Math. Soc. 129 (2001), 1891-1898

[65] P. Schauenburg: On the Frobenius-Schur indicators for quasi-Hopf algebras, J. Algebra 282 (2004), 129-139

[66] J. P. Serre: Local fields, Grad. Texts Math., Vol. 67, Springer, Berlin, 1979

[67] Y. Sommerhäuser: Ribbon transformations, integrals, and triangular decompositions, J. Algebra 282 (2004), 423-489

[68] Y. Sommerhäuser/Y. Zhu: Hopf algebras and congruence subgroups, Preprint, arXiv:0710.0705v2 [math.RA], 2008

[69] Y. Sommerhäuser/Y. Zhu: On the notion of a ribbon quasi-Hopf algebra, Preprint, 2009

[70] I. Schur: Über die Gaussschen Summen, Gött. Nachr. (1921), 147-153

[71] M. E. Sweedler: Integrals for Hopf algebras, Ann. Math., II. Ser., 89 (1969), 323-335

[72] M. E. Sweedler: Hopf algebras, W. A. Benjamin, New York, 1969

[73] V. G. Turaev: Quantum invariants of knots and 3-manifolds, de Gruyter Stud. Math., Vol. 18, de Gruyter, Berlin, 1994

[74] L. C. Washington: Introduction to cyclotomic fields, Grad. Texts Math., Vol. 83, Springer, Berlin, 1982

[75] S. J. Witherspoon: The representation ring and the centre of a Hopf algebra, Can. J. Math. 51 (1999), 881-896